Guía para desarrolladores

AWS Config

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Config: Guía para desarrolladores

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Config? ... 1
Consideraciones ... 1
Modos de utilizar AWS Config ... 1
Administración de recursos ... 2
Auditoría y conformidad ... 2
Administración y resolución de problemas de cambios de configuración ... 2
Análisis de seguridad ... 2
Soluciones conjuntas con socios ... 3
Características ... 3
Cómo AWS Config funciona ... 4
Detección de recursos ... 5
Seguimiento de recursos ... 5
Entrega de elementos de configuración ... 6
Controla el acceso a AWS Config ... 10
Terminología y conceptos ... 10
AWS Config Interfaces ... 11
Administración de recursos ... 12
Registro de configuración ... 13
Canal de entrega ... 6
AWS Config Reglas ... 15
Paquetes de conformidad ... 18
Agregadores ... 19
AWS Integraciones de servicios ... 20
AWS Organizations ... 20
AWS Control Tower ... 21
AWS CloudTrail ... 21
AWS Security Hub CSPM ... 21
AWS Trusted Advisor ... 22
AWS Audit Manager ... 22
AWS Systems Manager ... 23
AWS Firewall Manager ... 23
Hosts EC2 dedicados de Amazon ... 23
Equilibrador de carga de aplicación ... 24
AWS CodeBuild ... 24

AWS X-Ray ... 24
AWS Service Management Connector ... 25
Amazon API Gateway ... 25
Compatibilidad de la región ... 25
Consideraciones ... 25
Lista de regiones compatibles ... 26
Límites de los servicios ... 31
Información complementaria ... 33
AWS Kits de desarrollo de software para AWS Config ... 34
Introducción ... 36
Registrarse en AWS ... 36
Inscríbase en una Cuenta de AWS ... 36
Creación de un usuario con acceso administrativo ... 37
Formas de empezar AWS Config ... 38
Configuración de (consola) ... 38
Configuración ... 38
Configuración en un clic ... 39
Configuración manual ... 43
Configuración (AWS CLI) ... 50
Configuración ... 50
Requisitos previos ... 50
Inicio de AWS Config ... 121
Verificación de la configuración ... 125
Trabajando con AWS SDKs ... 127
Registro de configuración ... 129
Consideraciones sobre el registrador de configuración administrado por el cliente ... 130
Consideraciones sobre los registradores de configuración vinculados a servicios ... 131
Servicios admitidos ... 133
Detección de desviaciones para el registrador de configuración ... 134
Inicio del registrador de configuración administrado por el cliente ... 134
Detención del registrador de configuración administrado por el cliente ... 135
Cambio de la frecuencia de registro del registrador de configuración administrado por el cliente ... 136
Cambio del nombre del registrador de configuración administrado por el cliente ... 139
Visualización de los registradores de configuración ... 140
Eliminación de registradores de configuración ... 141

Canal de entrega ... 143
Consideraciones ... 143
Terminología ... 144
Componentes de un elemento de configuración ... 145
Visualización del canal de entrega ... 148
Actualización del canal de entrega ... 149
Cambio de nombre del canal de entrega ... 154
Entrega de instantáneas de configuración ... 155
Entrega de instantáneas de configuración ... 156
Verificación del estado de entrega ... 156
Visualización de instantáneas de configuración ... 157
Visualización de instantáneas de configuración ... 157
Instantánea de configuración de ejemplo ... 158
Notificaciones de ejemplo ... 163
Ejemplo de notificaciones de cambio de elemento de configuración ... 164
Ejemplo de notificación de entrega de historial de configuración ... 178
Ejemplo de notificación de inicio de entrega de instantánea de configuración ... 179
Ejemplo de notificación de entrega de instantánea de configuración ... 179
Ejemplo de notificación de cambio de conformidad ... 180
Ejemplo de notificación de inicio de evaluación de reglas ... 184
Ejemplo de notificación de cambio de elemento de configuración sobredimensionado ... 185
Ejemplo de notificación de entrega fallida ... 188
AWS Config Tablero ... 190
Cumplimiento e inventario de recursos ... 190
AWS Config Métricas de uso y éxito ... 192
Administración de recursos ... 196
Tipos de recursos admitidos ... 197
Amazon AppStream ... 198
Amazon AppFlow ... 199
Amazon AppIntegrations ... 199
Amazon API Gateway ... 199
Amazon Athena ... 201
Amazon Bedrock ... 201
Amazon CloudFront ... 202
Amazon CloudWatch ... 203
Amazon CodeGuru ... 204

Amazon Cognito 204
Amazon Comprehend 205
Amazon Connect 205
Amazon Detective 206
Amazon DynamoDB 207
Amazon EC2 207
Amazon ECR 217
Amazon ECS 218
Amazon EFS 219
Amazon EKS 220
Amazon EMR 220
Amazon EMR sin servidor 221
Amazon EventBridge 221
Amazon Forecast 222
Amazon Fraud Detector 222
Amazon GameLift 223
Amazon GuardDuty 223
Amazon Inspector 224
Amazon IVS 224
Amazon Keyspaces 225
Amazon Location Service 225
OpenSearch Servicio Amazon 226
Amazon Personalize 227
Amazon Pinpoint 227
Amazon QLDB 228
Amazon Kendra 229
Amazon Kinesis 229
Amazon Lex 230
Amazon Lightsail 230
Amazon Lookout for Metrics 231
Amazon Lookout for Vision 231
Amazon Macie 231
Amazon Managed Grafana 231
Servicio administrado por Amazon para Prometheus 232
Amazon MemoryDB 232
Amazon MQ 232

Amazon MSK 232
Amazon Quick 233
Amazon Redshift 234
Amazon RDS 236
Amazon Route 53 237
Amazon SageMaker AI 239
Amazon SES 242
Amazon SNS 243
Amazon SQS 243
Amazon S3 243
Amazon WorkSpaces 246
AWS Amplify 247
AWS AppConfig 247
AWS App Runner 248
AWS App Mesh 248
AWS AppSync 249
AWS Audit Manager 250
AWS Auto Scaling 250
AWS Intercambio de datos B2B 251
AWS Backup 251
AWS Batch 252
Administración de facturación y costos de AWS 253
AWS Budgets 253
AWS Certificate Manager 254
AWS Salas limpias 254
AWS CloudFormation 254
AWS CloudTrail 255
AWS Cloud9 255
AWS Cloud Map 256
AWS CodeArtifact 257
AWS CodeBuild 257
AWS CodeDeploy 258
AWS CodePipeline 258
AWS Config 259
AWS DMS 260
AWS DataSync 261

AWS Deadline Cloud 262
AWS Device Farm 263
AWS Elastic Beanstalk 263
AWS Entity Resolution 264
AWS FIS 265
AWS Global Accelerator 265
AWS Glue 265
AWS Ground Station 266
AWS HealthLake 267
AWS YO SOY 267
AWS IoT 269
AWS KMS 273
AWS Lambda 273
AWS Mainframe Modernization 274
AWS Network Firewall 274
AWS Network Manager 275
AWS Organizations 276
AWS Panorama 277
AWS Private CA 277
AWS Resilience Hub 278
Explorador de recursos de AWS 278
AWS RoboMaker 278
AWS Signer 279
AWS Secrets Manager 279
AWS Security Hub CSPM 280
AWS Service Catalog 280
AWS Shield 281
AWS Step Functions 281
AWS Systems Manager 282
AWS Transfer Family 283
AWS WAF 283
AWS X-Ray 286
Elastic Load Balancing 286
MediaConnect 287
MediaPackage 288
MediaPackage 289

MediaTailor ... 289
Cobertura de los recursos según la disponibilidad por región ... 290
América del Norte y del Sur ... 290
Europa ... 342
Asia Pacífico ... 385
China ... 443
África y Oriente Medio ... 467
GovCloud ... 501
AWS Recursos de grabación ... 528
Consideraciones ... 529
Recursos regionales y globales ... 530
AWS Config Reglas y tipos de recursos globales ... 533
Frecuencia de registro ... 535
Recursos no registrados ... 536
Registro de recursos (consola) ... 537
Recursos de grabación (AWS CLI) ... 540
Exclusión de recursos ... 548
Detención del registro ... 549
Registro de los recursos de terceros (AWS CLI) ... 549
Adición de recursos ... 550
Registro de elementos de configuración ... 554
Lectura de elementos de configuración ... 555
Eliminación de recursos ... 556
Registro de configuraciones de software ... 556
Requisitos previos ... 557
Registro de configuraciones de software ... 557
Búsqueda de recursos ... 559
Visualización de recursos ... 561
Visualización de la conformidad (consola) ... 561
Visualización del cumplimiento (AWS SDKs) ... 562
Visualización del historial de conformidad ... 570
Visualización del historial de conformidad (consola) ... 570
Visualización del historial de conformidad (AWS CLI) ... 571
Para recursos y reglas ... 577
Consulta del historial de conformidad ... 578
Etiquetado de recursos ... 579

Restricciones relacionadas con el etiquetado ... 580
Administración de las etiquetas con las acciones de la API de AWS Config ... 581
AWS Config Rules ... 582
Consideraciones ... 582
Compatibilidad de la región ... 585
Componentes de una regla ... 594
Cómo funcionan AWS Config las reglas ... 594
Tipos de desencadenadores ... 595
Modos de evaluación ... 597
Metadatos de las reglas ... 598
Reglas administradas ... 599
Lista de las reglas administradas ... 600
Lista de reglas administradas por modo de evaluación ... 1166
Lista de reglas administradas por tipo de desencadenador ... 1191
Lista de reglas administradas por disponibilidad regional ... 1216
Creación de reglas administradas con AWS CloudFormation plantillas ... 1830
Reglas personalizadas ... 1832
Reglas de políticas personalizadas ... 1832
Reglas de Lambda personalizadas ... 1832
Diferencias de formato para las reglas personalizadas AWS Config ... 1833
Creación de reglas de políticas personalizadas ... 1833
Creación de reglas de Lambda personalizadas ... 1840
Administración de los recursos eliminados para reglas de Lambda personalizadas de ... 1862
Roles vinculados a servicios de ... 1864
Reglas de la organización ... 1865
Consideraciones ... 1865
Implementación ... 1867
Compatibilidad de la región ... 1867
Adición de reglas ... 1872
Uso de la consola ... 1872
Uso del AWS SDKs ... 1875
Actualización de reglas ... 1880
Uso de la consola ... 1880
Uso del AWS SDKs ... 1881
Eliminación de reglas ... 1885
Consideraciones ... 1886

Uso de la consola ... 1886
Uso del AWS SDKs ... 1887
Visualización de reglas ... 1889
Uso de la consola ... 1889
Uso del AWS SDKs ... 1891
Activación de la evaluación proactiva ... 1903
Uso de la consola ... 1903
Uso del AWS SDKs ... 1906
Envío de evaluaciones a Security Hub (CSPM) ... 1910
Envíe las evaluaciones de las reglas a Security Hub (CSPM) ... 1910
Evaluación de recursos con reglas ... 1911
Eliminación de los resultados de evaluación ... 1915
Resolución de problemas ... 1916
Paquetes de conformidad ... 1919
Panel del paquete de conformidad ... 1920
Navegación por la página principal de los paquetes de conformidad ... 1920
Requisitos previos ... 1921
Paso 1: Comience a grabar AWS Config ... 1921
Paso 2: requisitos previos adicionales por tipo de paquete de conformidad ... 1921
Compatibilidad de la región ... 1927
Comprobaciones de procesos ... 1936
Plantilla de muestra ... 1937
Creación de comprobaciones de procesos ... 1938
Cambio en el estado de la conformidad ... 1938
Visualización y edición ... 1940
Plantillas de ejemplo del paquete de conformidad ... 1940
AWS Paquete de conformidad con las barandillas Control Tower Detective ... 1944
Prácticas recomendadas de ciberresiliencia para Amazon S3, Amazon EBS y Amazon DynamoDB ... 1945
Prácticas operativas recomendadas para cargas de trabajo de material de ABS CCIG 2.0 1945
Prácticas operativas recomendadas para cargas de trabajo estándar de ABS CCIG 2.0 ... 2187
Prácticas operativas recomendadas para ACSC Essential 8 ... 2366
Prácticas operativas recomendadas para ACSC ISM: parte 1 ... 2397
Prácticas operativas recomendadas para ACSC ISM: parte 2 ... 2550
Prácticas operativas recomendadas para IA y ML ... 2559
Prácticas operativas recomendadas para Amazon API Gateway ... 2559

Mejores prácticas operativas para Amazon CloudWatch 2560
Prácticas operativas recomendadas para Amazon DynamoDB 2560
Prácticas operativas recomendadas para Amazon S3 2560
Prácticas operativas recomendadas para APRA CPG 234 2560
Prácticas operativas recomendadas para la gestión de activos 2812
Mejores prácticas operativas para AWS Backup 2812
Prácticas operativas recomendadas para AWS Identity and Access Management 2812
Mejores prácticas operativas para el pilar de confiabilidad de AWS un marco de trabajo bien diseñado 2812
Mejores prácticas operativas para el pilar de seguridad de AWS Well-Architected Framework 2887
Prácticas operativas recomendadas para BCP y DR 3085
Mejores prácticas operativas para BNM T RMi 3086
Prácticas operativas recomendadas para el Perfil medio de control de la nube del Centro Canadiense de Ciberseguridad (CCCS) 3436
Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4 Level 1 5118
Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4 Level 2 5162
Mejores prácticas operativas para los controles de seguridad críticos de CIS v8 IG1 5221
Mejores prácticas operativas para los controles de seguridad críticos de CIS v8 IG2 5333
Mejores prácticas operativas para los controles de seguridad críticos de CIS v8 IG3 5529
Prácticas operativas recomendadas para los 20 principales controles del CIS 5742
Prácticas operativas recomendadas para CISA Cyber Essentials 5830
Prácticas operativas recomendadas para los Servicios de Información de la Justicia Criminal (CJIS, por sus siglas en inglés) 6061
Prácticas operativas recomendadas para la CMMC 2.0 de nivel 1 6206
Prácticas operativas recomendadas para la CMMC 2.0 de nivel 2 6341
Prácticas operativas recomendadas para servicios de computación 6795
Prácticas operativas recomendadas para la resiliencia de datos 6796
Prácticas operativas recomendadas para servicios de bases de datos 6796
Prácticas operativas recomendadas para lagos de datos y servicios de análisis 6796
Mejores prácticas operativas para DevOps 6797
Prácticas operativas recomendadas para EC2 6797
Prácticas operativas recomendadas para el cifrado y la administración de claves 6797
Prácticas operativas recomendadas para la guía de ciberseguridad para pymes de la ENISA 6797
Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Bajo 7024

Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Medio 7145
Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Alto . 7282
Prácticas operativas recomendadas para la FDA Título 21 CFR Parte 11 7425
Prácticas operativas recomendadas para el FedRAMP (bajo) 7869
Prácticas operativas recomendadas para FedRAMP (moderadas) 8177
Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 1) 8798
Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 2) 9478
Prácticas operativas recomendadas para FFIEC 9629
Catálogo de criterios de cumplimiento de las prácticas recomendadas operativas para la computación en la nube en Alemania (C5) 9884
Prácticas recomendadas operativas para la Ley Gramm Leach Bliley (GLBA) 9987
Prácticas operativas recomendadas para el anexo 11 de la UE de GxP 10046
Prácticas operativas recomendadas para la seguridad de la HIPAA 10226
Prácticas operativas recomendadas para IRS 1075 10780
Prácticas operativas recomendadas para K-ISMS 11028
Prácticas operativas recomendadas para el equilibrado de carga 11124
Prácticas operativas recomendadas para el registro 11124
Prácticas operativas recomendadas para servicios de administración y gobernanza 11124
Prácticas operativas recomendadas para MAS Notice 655 11124
Prácticas operativas recomendadas para MAS TRMG 11169
Prácticas operativas recomendadas para el monitoreo 11419
Prácticas operativas recomendadas para NBC TRMG 11419
Prácticas operativas recomendadas para NERC CIP BCSI 12013
Prácticas operativas recomendadas para los NCSC Cloud Security Principles 12086
Prácticas operativas recomendadas para el NCSC Cyber Assesment Framework 12213
Prácticas operativas recomendadas para redes y servicios de entrega de contenido 12420
Prácticas operativas recomendadas para el NIST 800-53 rev 4 12420
Prácticas operativas recomendadas para el NIST 800-53 rev 5 12789
Prácticas operativas recomendadas para NIST 800 171 13539
Prácticas operativas recomendadas para NIST 800 172 13924
Prácticas operativas recomendadas para NIST 800 181 14006
Prácticas operativas recomendadas para NIST 1800 25 14587
Prácticas operativas recomendadas para el NIST CSF 14770
Prácticas operativas recomendadas para el NIST Privacy Framework v1.0 15186
Prácticas operativas recomendadas para NYDFS 23 15461

Prácticas operativas recomendadas para NZISM 3.8 15673
Prácticas operativas recomendadas para el PCI DSS 3.2.1 15841
Prácticas operativas recomendadas para el PCI DSS 4.0 (excluye los tipos de recursos globales) 16215
Prácticas operativas recomendadas para el PCI DSS 4.0 (incluye los tipos de recursos globales) 16573
Prácticas operativas recomendadas para recursos de acceso público 17009
Mejores prácticas operativas para el marco de ciberseguridad del RBI para UCBs 17009
Prácticas operativas recomendadas para RBI MD-ITF 17065
Prácticas operativas recomendadas para los servicios de seguridad, identidad y conformidad 17235
Prácticas operativas recomendadas para soluciones sin servidor 17235
Prácticas operativas recomendadas para servicios de almacenamiento 17235
Prácticas operativas recomendadas para el SWIFT CSP 17236
Prácticas de seguridad recomendadas para Amazon Elastic Container Service (Amazon ECS) 17275
Prácticas de seguridad recomendadas para Amazon Elastic File System (Amazon EFS) 17276
Prácticas de seguridad recomendadas para Amazon Elastic Kubernetes Service (Amazon EKS) 17276
Mejores prácticas de seguridad para Amazon CloudFront 17276
Mejores prácticas de seguridad para Amazon OpenSearch Service 17276
Prácticas de seguridad recomendadas para Amazon Redshift 17277
Prácticas de seguridad recomendadas para Amazon Relational Database Service (Amazon RDS) 17277
Mejores prácticas de seguridad para AWS Auto Scaling 17277
Mejores prácticas de seguridad para AWS CloudTrail 17278
Mejores prácticas de seguridad para AWS CodeBuild 17278
Prácticas recomendadas de seguridad para Amazon ECR 17278
Mejores prácticas de seguridad para AWS Lambda 17278
Mejores prácticas de seguridad para AWS Network Firewall 17279
Prácticas de seguridad recomendadas para Amazon SageMaker AI 17279
Mejores prácticas de seguridad para AWS Secrets Manager 17279
Mejores prácticas de seguridad para AWS WAF 17279
Plantillas de ejemplo con acción de corrección 17280
Creación de plantillas personalizadas 17280
Terminología 17280

Personalización de la plantilla 17281
Implementación de paquetes de conformidad 17285
Edición de paquetes de conformidad 17288
Eliminación de paquetes de conformidad 17290
Consideraciones 17290
Cómo eliminar un paquete de conformidad 17291
Visualización de paquetes de conformidad 17292
Visualización del historial de conformidad 17295
Visualización de la línea de tiempo de conformidad 17296
Consulta del historial de conformidad 17296
Administración de paquetes de conformidad de la organización 17298
Consideraciones 17298
Implementación 17300
Compatibilidad de la región 17300
Solución de problemas 17305
Estado fallido de un paquete de conformidad 17305
Reglas colgantes en un paquete de conformidad 17306
Corrección 17309
Compatibilidad de la región 17309
Configuración de la corrección manual 17313
Configuración de la corrección automática 17315
Eliminación de acciones correctivas 17317
Agregadores 17319
Casos de uso 17319
Terminología 17320
Compatibilidad de la región 17320
Panel del agregador 17325
Uso del panel del agregador 17325
Panel de cumplimiento 17328
Panel de inventario 17331
Creación de agregadores 17333
Registro de un administrador delegado 17339
Edición de agregadores 17341
Eliminación de agregadores 17343
Autorización de cuentas de agregador 17343
Consideraciones 17344

Autorización de envío 17344
Eliminación de autorizaciones 17346
Consideraciones 17346
Eliminación de la autorización 17347
Visualización de agregadores 17347
Resolución de problemas 17349
Consultas avanzadas 17351
Características 17352
Componentes de las consultas 17352
Sinopsis 17352
Parámetros 17353
Ejemplos 17353
Editor de consultas (consola) 17354
Consideraciones 17354
Utilice un AWS ejemplo de consulta 17354
Creación de una consulta personalizada 17355
Editor de consultas (AWS CLI) 17356
Consideraciones 17356
Consulta de los datos de configuración de los recursos 17357
Guardar una consulta 17359
Ver todas las consultas guardadas 17359
Obtener detalles de una consulta guardada 17360
Eliminar una consulta guardada 17360
Procesador de consultas en lenguaje natural 17361
Consideraciones 17361
Consultas mediante el procesador de consultas en lenguaje natural 17354
Ejemplos de peticiones 17363
Aportación de comentarios 17366
Compatibilidad de la región 17367
Consultas de ejemplo 17367
Ejemplos de consultas de relación 17373
Limitaciones 17375
Rango CIDR notation/IP 17377
Múltiples propiedades en una matriz 17377
Compatibilidad de la región 17378
Eliminación de datos de 17384

Configuración de periodo de retención de datos (consola) 17386
Seguridad 17388
Protección de los datos 17389
Cifrado de datos en tránsito 17390
Cifrado de datos en tránsito 17390
Gestión de identidad y acceso 17390
Público 17391
Autenticación con identidades 17391
Administración del acceso con políticas 17392
¿Cómo AWS Config funciona con IAM 17394
Ejemplos de políticas basadas en identidades 17400
AWS políticas gestionadas 17419
Permisos para el rol de IAM 17606
Actualización del rol de IAM 17610
Permisos para el bucket de Amazon S3 17612
Permisos para la clave de KMS 17616
Permisos para el tema de Amazon SNS 17619
Resolución de problemas 17623
Uso de roles vinculados a servicios 17625
Respuesta frente a incidencias 17627
Validación de la conformidad 17628
Resiliencia 17628
Seguridad de infraestructuras 17629
Configuración y análisis de vulnerabilidades 17629
Prevención de la sustitución confusa entre servicios 17629
Prácticas recomendadas 17630
Registro y supervisión 17631
Registro 17631
AWS Config Información en CloudTrail 17631
Descripción de las entradas de los archivos de AWS Config registro 17633
Ejemplos de archivos de registro 17633
Supervisión 17641
Uso de Amazon SQS 17641
Uso de Amazon EventBridge 17644
Puntos de conexión de VPC de Amazon 17651
Crear un punto de enlace de la VPC 17651

FAQs 17652
No puedo ver los últimos cambios de configuración 17652
¿Debería poder ver los cambios de configuración de inmediato? 17652
Relaciones indirectas en AWS Config 17652
¿Qué es una relación de recursos? 17652
¿Qué es una relación directa e indirecta con respecto a un recurso? 17653
¿Qué relaciones indirectas AWS Config admite? 17654
¿Qué escenarios utilizan relación indirecta? 17655
¿Cómo se crean los elementos de configuración según la relación directa e indirecta? ... 17657
¿Cuáles son los elementos de configuración que se generan por las relaciones indirectas? 17658
¿Cómo deshabilito la relación indirecta? 17659
¿Cómo puedo obtener los datos de configuración vinculados con las relaciones indirectas? 17660
Ejemplos de código 17661
Conceptos básicos 17662
Acciones 17662
Historial de documentos 17701
Actualizaciones anteriores 17870
..... 17945

¿Qué es AWS Config?

AWS Config proporciona una vista detallada de la configuración de los recursos de AWS de su cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.

Un recurso de AWS es una entidad con la que se puede trabajar en AWS, como una instancia de Amazon Elastic Compute Cloud (EC2), un volumen de Amazon Elastic Block Store (EBS), un grupo de seguridad o una Amazon Virtual Private Cloud (Amazon VPC). Para obtener una lista completa de los recursos de AWS admitidos por AWS Config, consulte Tipos de recursos compatibles para AWS Config.

Consideraciones

- Cuenta de AWS: necesita una Cuenta de AWS activa. Para obtener más información, consulte Signing up for AWS.
- Bucket de Amazon S3: necesita un bucket de S3 para recibir datos de las instantáneas y el historial de configuración. Para obtener más información, consulte Permisos para el bucket de Amazon S3.
- Tema de Amazon SNS: necesita un Amazon SNS para recibir notificaciones cuando haya cambios en las instantáneas y el historial de la configuración. Para obtener más información, consulte Permissions for the Amazon SNS Topic.
- Rol de IAM: necesita un rol de IAM que tenga los permisos necesarios para obtener acceso a AWS Config. Para obtener más información, consulte Permissions for the IAM Role.
- Tipos de recursos: puede decidir qué tipos de recursos desea que AWS Config registre. Para obtener más información, consulte Recording AWS Resources.

Modos de utilizar AWS Config

Cuando ejecuta sus aplicaciones en AWS, normalmente utiliza recursos de AWS que debe crear y administrar colectivamente. A medida que sigue aumentando la demanda de su aplicación, también lo hace la necesidad de realizar un seguimiento de sus recursos de AWS. AWS Config se ha diseñado para ayudarle a supervisar sus recursos de la aplicación en los siguientes casos:

Administración de recursos

Para ejercer un mejor control de las configuraciones de sus recursos y detectar configuraciones erróneas de los mismos, necesita una visibilidad minuciosa sobre los recursos que existen y cómo dichos recursos están configurados en cualquier momento. Puede utilizar AWS Config para que se le notifique cuando se crean, modifican o eliminan recursos sin tener que supervisar estos cambios sondeando las llamadas realizadas a cada recurso.

Puede utilizar reglas de AWS Config para evaluar los ajustes de configuración de sus recursos de AWS. Cuando AWS Config detecta que un recurso infringe las condiciones en una de las reglas,AWS Config marca el recurso como no conforme y envía una notificación. AWS Config evalúa continuamente los recursos a medida que se crean, modifican o eliminan.

Auditoría y conformidad

Es posible que trabaje con datos que requieren auditorías frecuentes para garantizar la conformidad con las políticas internas y las prácticas recomendadas. Para demostrar la conformidad, necesita acceder a las configuraciones históricas de los recursos. Esta información la proporciona AWS Config.

Administración y resolución de problemas de cambios de configuración

Al utilizar varios recursos de AWS que dependen unos de otros, un cambio en la configuración de un recurso podría tener consecuencias imprevistas en los recursos relacionados. Con AWS Config, puede ver cómo el recurso que va a modificar está relacionado con otros recursos y evaluar el impacto del cambio.

También puede utilizar las configuraciones históricas de los recursos proporcionadas por AWS Config para solucionar problemas y para acceder a la última configuración correcta conocida de un recurso con problemas.

Análisis de seguridad

Para analizar posibles problemas de seguridad, necesita información histórica detallada sobre las configuraciones de los recursos de AWS, como los permisos de AWS Identity and Access Management (IAM) que se otorgan a los usuarios, o las reglas de grupo de seguridad de Amazon EC2 que controlan el acceso a los recursos.

Puede utilizar AWS Config para ver la política de IAM que se ha asignado a un usuario, grupo o rol en cualquier momento en el que AWS Config ha estado registrando. Esta información puede

ayudarle a determinar los permisos que pertenecían a un usuario en un momento específico: por ejemplo, puede ver si el usuario `John Doe` tenía permiso para modificar los ajustes de el 1 de enero de 2015.

También puede utilizar AWS Config para ver la configuración de los grupos de seguridad de EC2, incluidas las reglas de puertos que estaban abiertas en un momento concreto. Esta información puede ayudarle a determinar si un grupo de seguridad ha bloqueado el tráfico entrante de TCP a un puerto específico.

Soluciones conjuntas con socios

AWS colabora con terceros especialistas en el registro y análisis para proporcionar soluciones que usan la información de AWS Config. Para obtener más información, visite la página de información detallada de AWS Config en AWS Config.

Características

Al configurar AWS Config, puede completar lo siguiente:

Administración de recursos

- Especificar los tipos de recursos que desea que registre AWS Config.

- Configure un bucket de Amazon S3 para recibir una instantánea de configuración a solicitud y el historial de configuración.
- Configure un tema de Amazon SNS para enviar notificaciones del flujo de configuración.
- Conceda a AWS Config los permisos que necesita para acceder al bucket de Amazon S3 y el tema de SNS.

  Para obtener más información, consulte Visualización de historial y configuraciones de recursos de AWS y Administración del historial y las configuraciones de los recursos de AWS.

Reglas y paquetes de conformidad

- Especifique las reglas que desea que utilice AWS Config para evaluar la información de conformidad para los tipos de recursos registrados.
- Use paquetes de conformidad o un conjunto de reglas que se puedan implementar y supervisar como una sola entidad en la Cuenta de AWS.

Para obtener más información, consulte Evaluación de recursos con reglas de AWS Config y Paquetes de conformidad.

Corrección

- Corrija los recursos no conformes evaluados por Reglas de AWS Config.

  Para obtener más información, consulte Remediation.

Agregadores

- Utilice un agregador para obtener una vista centralizada del inventario de recursos y de la conformidad. Un agregador recopila datos de conformidad y configuración de AWS Config desde distintas Cuentas de AWS y regiones de AWS, y los agrupa en una sola cuenta y región.

  Para obtener más información, consulte Acumulación de datos de varias cuentas y regiones.

Consultas avanzadas

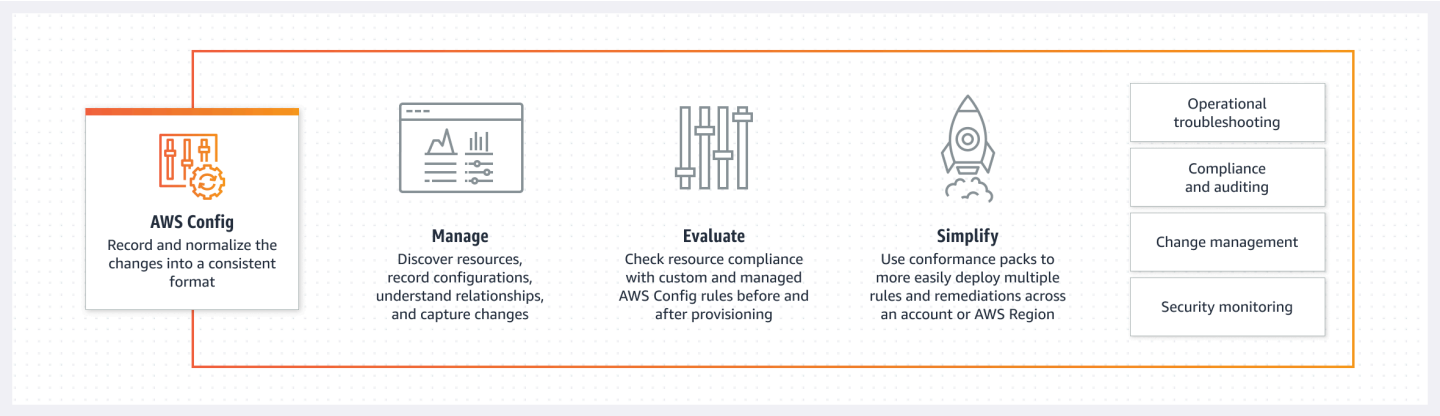
- Utilice una de las consultas de ejemplo o escriba la suya propia consultando el esquema de configuración del recurso AWS.

  Para obtener más información, consulte Consulta del estado de configuración actual de los recursos de AWS.

Cómo AWS Config funciona

AWS Config proporciona una vista detallada de la configuración de AWS los recursos de su AWS cuenta. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.

Un AWS recurso es una entidad con la que puede trabajar AWS, como una instancia de Amazon Elastic Compute Cloud (EC2), un volumen de Amazon Elastic Block Store (EBS), un grupo de seguridad o una Amazon Virtual Private Cloud (VPC). Para obtener una lista completa de AWS los recursos compatibles AWS Config, consulte. Tipos de recursos compatibles para AWS Config



Detección de recursos

Al activarlo AWS Config, primero descubre los AWS recursos compatibles que existen en tu cuenta y genera un elemento de configuración para cada recurso.

AWS Config también genera elementos de configuración cuando cambia la configuración de un recurso y mantiene registros históricos de los elementos de configuración de los recursos desde el momento en que se inicia el registrador de configuración. De forma predeterminada, AWS Config crea elementos de configuración para todos los recursos compatibles de la región. Si no desea AWS Config crear elementos de configuración para todos los recursos compatibles, puede especificar los tipos de recursos de los que quiere que haga un seguimiento.

Antes de especificar el tipo de recurso del que se AWS Config va a realizar el seguimiento, compruebe la cobertura de los recursos por región y la disponibilidad para comprobar si el tipo de recurso es compatible con la AWS región en la que va a realizar la configuración AWS Config. Si al menos una región admite un tipo de recurso, puede habilitar el registro de ese tipo de recurso en todas las regiones compatibles AWS Config, incluso si el tipo de recurso especificado no es compatible con la AWS región en la que está configurando AWS Config. AWS Config

Seguimiento de recursos

AWS Config realiza un seguimiento de todos los cambios en sus recursos mediante la llamada a la API Describe o List para cada recurso de su cuenta. El servicio utiliza las mismas llamadas al API para capturar los detalles de la configuración de todos los recursos relacionados.

Por ejemplo, al eliminar una regla de salida de un grupo de seguridad de VPC, se invoca una AWS Config llamada a la API Describe en el grupo de seguridad. AWS Config a continuación, invoca una llamada a la API Describe en todas las instancias asociadas al grupo de seguridad. Las configuraciones actualizadas del grupo de seguridad (el recurso) y de cada instancia (los

recursos relacionados) se registran como elementos de configuración y se entregan en un flujo de configuración en un bucket de Amazon Simple Storage Service (Amazon S3).

AWS Config también realiza un seguimiento de los cambios de configuración que no fueron iniciados por la API. AWS Config examina las configuraciones de los recursos periódicamente y genera elementos de configuración para las configuraciones que han cambiado.

Si utiliza AWS Config reglas, evalúa AWS Config continuamente las configuraciones de los AWS recursos para determinar la configuración deseada. Según la regla, AWS Config evaluará sus recursos en respuesta a los cambios de configuración o de forma periódica. Cada regla está asociada a una función AWS Lambda que contiene la lógica de evaluación de la regla. Al AWS Config evaluar los recursos, invoca la función de la AWS Lambda regla. La función devuelve el estado de conformidad de los recursos evaluados. Si un recurso infringe las condiciones de una regla, AWS Config marca el recurso y la regla como no conformes. Cuando el estado de conformidad de un recurso cambia, AWS Config envía una notificación a tu tema de Amazon SNS.

Entrega de elementos de configuración

AWS Config puede entregar elementos de configuración a través de uno de los siguientes canales:

Bucket de Amazon S3

AWS Config realiza un seguimiento de los cambios en la configuración de sus AWS recursos y envía periódicamente los detalles de configuración actualizados a un bucket de Amazon S3 que especifique. Para cada tipo de recurso que AWS Config registra, envía un archivo de historial de configuración cada seis horas. Cada archivo de historial de configuración contiene información sobre los recursos que han cambiado en ese periodo de seis horas. Cada archivo incluye recursos de un tipo, como instancias de Amazon EC2 o volúmenes de Amazon EBS. Si no se produce ningún cambio en la configuración, AWS Config no envía ningún archivo.

AWS Config envía una instantánea de la configuración a su bucket de Amazon S3 cuando utiliza el deliver-config-snapshotcomando con la AWS CLI o cuando utiliza la DeliverConfigSnapshotacción con la AWS Config API. Una instantánea de configuración contiene los detalles de la configuración de todos los recursos que AWS Config registra en la cuenta de Cuenta de AWS. El archivo de historial de configuración y la instantánea de configuración están en formato JSON.

> **Note**
>
> AWS Config solo entrega los archivos del historial de configuración y las instantáneas de configuración al bucket de S3 especificado; AWS Config no modifica las políticas del ciclo de

vida de los objetos del bucket de S3. Puede usar políticas de ciclo de vida para especificar si desea eliminar o archivar objetos en Amazon Glacier. Para obtener más información, consulte Administración de la configuración del ciclo de vida en la Guía del usuario de Amazon Simple Storage Service. También puede consultar la publicación del blog Archiving Amazon S3 Data to Amazon Glacier.

Tema de Amazon SNS

Un tema de Amazon Simple Notification Service (Amazon SNS) es un canal de comunicación que utiliza para entregar mensajes (o notificaciones) a puntos de enlace de suscripción, como una dirección de correo electrónico o un cliente. Entre otros tipos de notificaciones de Amazon SNS se incluyen mensajes de notificación de inserción para aplicaciones en teléfonos móviles, notificaciones por SMS (servicio de mensajes cortos) a teléfonos y smartphones habilitados para SMS y solicitudes HTTP POST. Para obtener los mejores resultados, utilice Amazon SQS como punto de conexión de notificación para el tema de SNS y, a continuación, procese la información en la notificación de forma programada.

AWS Config usa el tema Amazon SNS que especifiques para enviarte las notificaciones. El tipo de notificación que está recibiendo se indica por el valor de la clave `messageType` en el cuerpo del mensaje, como en el siguiente ejemplo:

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

Las notificaciones pueden ser cualquiera de los siguientes tipos de mensajes.

Tipo de mensaje	Descripción
ComplianceChangeNotification	El tipo de conformidad del recurso que AWS Config evalúa ha cambiado. El tipo de conformidad indica si el recurso cumple con una AWS Config regla específica y se representa mediante la `ComplianceType` clave del mensaje. El mensaje incluye objetos `newEvaluationResult` y `oldEvaluationResult` de comparación.

Tipo de mensaje	Descripción
ConfigRulesEvaluationStarted	AWS Config comenzó a evaluar la regla en función de los recursos especificados.
ConfigurationSnapshotDeliveryStarted	AWS Config comenzó a entregar la instantán ea de configuración a su bucket de Amazon S3. Se proporciona el nombre del bucket de Amazon S3 para la clave `s3Bucket` en el mensaje.
ConfigurationSnapshotDeliveryCompleted	AWS Config entregó correctamente la instantán ea de configuración a su bucket de Amazon S3.
ConfigurationSnapshotDeliveryFailed	AWS Config no se pudo entregar la instantánea de configuración a su bucket de Amazon S3.
ConfigurationHistoryDeliveryCompleted	AWS Config entregó correctamente el historial de configuración a su bucket de Amazon S3.
ConfigurationItemChangeNotification	Un recurso se ha creado, eliminado o cambiado en la configuración. Este mensaje incluye los detalles del elemento de configura ción que se AWS Config crea para este cambio e incluye el tipo de cambio. Estas notificaciones se entregan en cuestión de minutos tras el cambio y se conocen colectivamente como el flujo de configuración.

Tipo de mensaje	Descripción
OversizedConfigurationItemChangeNotification	Este tipo de mensaje se entrega cuando una notificación de cambio de elemento de configuración supera el tamaño máximo permitido por Amazon SNS. El mensaje incluye un resumen del elemento de configuración. A excepción de los mensajes SMS, los mensajes de Amazon SNS pueden contener hasta 256 KB de datos de texto, incluidos XML, JSON y texto sin formato. Puede ver la notificación completa en el bucket de Amazon S3 especific ado.
OversizedConfigurationItemChangeDeli veryFailed	AWS Config no se pudo entregar la notificac ión de cambio del elemento de configuración sobredimensionado a su bucket de Amazon S3.

Para obtener ejemplos de notificaciones, consulte Notificaciones que se AWS Config envían a un tema de Amazon SNS. Para obtener más información sobre Amazon SNS, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

> **Note**
>
> ¿Por qué no puedo ver los cambios de configuración más recientes?
> AWS Config por lo general, registra los cambios de configuración de sus recursos inmediatamente después de detectar un cambio o con la frecuencia que usted especifique. Aunque el sistema hace todo lo posible porque sea así, a veces puede tardar más tiempo. Si los problemas persisten después de un tiempo, ponte en contacto con Amazon Soportey proporciona tus AWS Config estadísticas compatibles CloudWatch. Para obtener más información sobre estas métricas, consulte AWS Config Usage and Success Metrics.

Controla el acceso a AWS Config

AWS Identity and Access Management es un servicio web que permite a los clientes de Amazon Web Services (AWS) gestionar los usuarios y los permisos de los usuarios.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .
- Usuarios gestionados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

AWS Config terminología y conceptos

Para ayudarle a entender AWS Config, en este tema se explican algunos de los conceptos clave.

Contenido

- AWS Config Interfaces
  - AWS Config Consola
  - AWS Config CLI
  - AWS Config APIs
  - AWS Config SDKs
- Administración de recursos
  - AWS Recursos
  - Relación de recursos

- Registro de configuración
- Canal de entrega
  - Elementos de configuración
  - Historial de configuración
  - Instantánea de configuración
  - Flujo de configuración
- AWS Config Reglas
  - Resultados de la evaluación
  - Tipos de regla
  - Tipos de desencadenadores
  - Modos de evaluación
- Paquetes de conformidad
- Acumulación de datos de varias cuentas y regiones
  - Cuenta de origen
  - Región de origen
  - Agregador
  - Agregador vinculado a servicios
  - Cuenta de agregador
  - Autorización

AWS Config Interfaces

AWS Config Consola

Puede gestionar el servicio mediante la AWS Config consola. Para obtener más información acerca de Consola de administración de AWS, consulte Consola de administración de AWS.

AWS Config CLI

AWS Command Line Interface Es una herramienta unificada con la que puede interactuar AWS Config desde la línea de comandos. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface. Para obtener una lista completa de los comandos de AWS Config CLI, consulte Comandos disponibles.

AWS Config APIs

Además de la consola y la CLI, también puede utilizarlas AWS Config RESTful APIs para programar AWS Config directamente. Para obtener más información, consulte la Referencia de la API de AWS Config.

AWS Config SDKs

Como alternativa al uso de la AWS Config API, puede utilizar una de las AWS SDKs. Cada SDK se compone de bibliotecas y código de muestra para diversos lenguajes de programación y plataformas. SDKs Proporcionan una forma cómoda de crear un acceso programático a AWS Config. Por ejemplo, puede utilizarlos SDKs para firmar las solicitudes de forma criptográfica, gestionar los errores y volver a intentar las solicitudes automáticamente. A fin de obtener más información, consulte la página de Herramientas para Amazon Web Services.

Administración de recursos

Comprender los componentes básicos de AWS Config le ayudará a realizar un seguimiento del inventario y los cambios de los recursos y a evaluar las configuraciones de los recursos. AWS

AWS Recursos

AWS los recursos son entidades que se crean y administran mediante las Consola de administración de AWS herramientas AWS Command Line Interface (CLI) o AWS asociadas. AWS SDKs Entre los ejemplos de AWS recursos se incluyen las instancias de Amazon EC2, los grupos de seguridad VPCs, Amazon y Amazon Elastic Block Store. AWS Config hace referencia a cada recurso mediante su identificador único, como el ID del recurso o un nombre de recurso de Amazon (ARN). Para obtener una lista de los tipos de recursos AWS Config compatibles, consulteTipos de recursos compatibles para AWS Config.

Relación de recursos

AWS Config descubre AWS los recursos de su cuenta y, a continuación, crea un mapa de relaciones entre AWS los recursos. Por ejemplo, una relación podría incluir un volumen de Amazon EBS `vol-123ab45d` adjunto a una instancia de Amazon EC2 `i-a1b2c3d4` que está asociada al grupo de seguridad `sg-ef678hk`.

Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.

Registro de configuración

El registrador de configuración almacena los cambios de configuración en los tipos de recursos incluidos en el ámbito como elementos de configuración (CI). Para obtener más información, consulte Uso del registrador de configuración.

Existen dos tipos de registradores de configuración.

Tipo	Descripción
Registrador de configuración administrado por el cliente	Un registrador de configuración que administr a usted. Usted establece los tipos de recursos incluidos en el ámbito. De forma predeterm inada, un grabador de configuración gestionad o por el cliente registra todos los recursos compatibles en el Región de AWS lugar en el que AWS Config se están ejecutando.
Registrador de configuración vinculado a servicios	Un grabador de configuración que está vinculado a un registro específico Servicio de AWS. Los tipos de recursos incluidos en el ámbito los establece el servicio vinculado.

Canal de entrega

Como registra AWS Config continuamente los cambios que se producen en sus AWS recursos, envía notificaciones y estados de configuración actualizados a través del canal de entrega. Puede administrar el canal de entrega para controlar dónde se AWS Config envían las actualizaciones de configuración.

Elementos de configuración

Un elemento de configuración representa una point-in-time vista de los distintos atributos de un AWS recurso compatible que existe en su cuenta. Los componentes de un elemento de configuración incluyen los metadatos, los atributos, las relaciones, la configuración actual y los eventos relacionados. AWS Config crea un elemento de configuración cada vez que detecta un cambio en un tipo de recurso que está registrando. Por ejemplo, si AWS Config está grabando buckets de Amazon S3, AWS Config crea un elemento de configuración cada vez que se crea,

actualiza o elimina un bucket. También puede seleccionar AWS Config crear un elemento de configuración con la frecuencia de grabación que haya establecido.

Para obtener más información, consulte Components of a Configuration Item y Recording Frequency.

Historial de configuración

Un historial de configuración es una colección de elementos de configuración de un recurso determinado durante cualquier periodo de tiempo. Un historial de configuración puede ayudarle a responder preguntas sobre, por ejemplo, cuándo se creó el recurso, cómo se ha configurado durante el último mes y qué cambios de configuración se introdujeron ayer a las 9 de la mañana. El historial de configuración está disponible en varios formatos. AWS Config entrega automáticamente un archivo de historial de configuración para cada tipo de recurso que se registre en un bucket de Amazon S3 que especifique. Puede seleccionar un recurso determinado en la AWS Config consola y navegar hasta todos los elementos de configuración anteriores de ese recurso utilizando la cronología. Asimismo, puede obtener acceso a los elementos de configuración históricos de un recurso desde la API.

Para obtener más información, consulte Viewing Compliance History y Querying Compliance History.

Instantánea de configuración

Una instantánea de configuración es una colección de elementos de configuración de los recursos admitidos que existen en su cuenta. Esta instantánea de configuración es una imagen completa de los recursos que se registran y sus configuraciones. La instantánea de configuración puede ser una herramienta útil para validar la configuración. Por ejemplo, puede examinar la instantánea de configuración con regularidad para los recursos que se han configurado de forma incorrecta o que potencialmente no deban existir. La instantánea de configuración está disponible en varios formatos. Puede hacer que la instantánea de configuración se entregue al bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Además, puede seleccionar un punto en el tiempo en la AWS Config consola y navegar por la instantánea de los elementos de configuración utilizando las relaciones entre los recursos.

Para obtener más información, consulte Delivering Configuration Snapshots, Viewing Configuration Snapshots y Example Configuration Snapshot.

Flujo de configuración

Un flujo de configuración es una lista que se actualiza automáticamente de todos los elementos de configuración de los recursos que AWS Config se están registrando. Cada vez que se crea,

se modifica o se elimina un recurso, AWS Config crea un elemento de configuración y lo añade al flujo de configuración. El flujo de configuración utiliza el tema de Amazon Simple Notification Service (Amazon SNS) de su elección. El flujo de configuración es útil para observar los cambios de configuración a medida que se producen y detectar posibles problemas, generar notificaciones si se modifican determinados recursos o actualizar los sistemas externos que deben reflejar la configuración de AWS los recursos.

AWS Config Reglas

Una AWS Config regla es una comprobación de conformidad que le ayuda a gestionar los ajustes de configuración ideales para AWS recursos específicos. AWS Config evalúa si las configuraciones de sus recursos cumplen con las normas pertinentes y muestra los resultados de conformidad.

Resultados de la evaluación

Hay cuatro posibles resultados de evaluación para una AWS Config regla.

Resultado de la evaluación	Descripción
`COMPLIANT`	La regla cumple las condiciones de la comprobación de cumplimiento.
`NON_COMPLIANT`	La regla no cumple las condiciones de la comprobación de cumplimiento.
`ERROR`	Uno de los required/optional parámetros no es válido, no es del tipo correcto o tiene un formato incorrecto.
`NOT_APPLICABLE`	Se utiliza para filtrar los recursos a los que no se puede aplicar la lógica de la regla. Por ejemplo, la alb-desync-mode-checkregla solo comprueba los balanceadores de carga de aplicaciones e ignora los balanceadores de carga de red y de puerta de enlace.

Tipos de regla

Hay dos tipos de reglas: Para obtener más información sobre la estructura de las definiciones y los metadatos de las reglas, consulte Componentes de una regla. AWS Config

Tipo	Descripción	Más información
Reglas administradas	Reglas predefinidas y personalizables creadas por AWS Config.	Para obtener una lista de reglas administradas, consulte Lista de reglas AWS Config administradas.
Reglas personalizadas	Reglas que usted crea desde cero. Hay dos formas de crear reglas AWS Config personalizadas: funciones Lambda (Guía para AWS Lambda desarrolladores) y Guard (Guard Repository) GitHub	Para obtener más información, consulte Creación de reglas de políticas AWS Config personalizadas y Creación de reglas Lambda AWS Config personalizadas.

Tipos de desencadenadores

Tras añadir una regla a su cuenta, AWS Config compara sus recursos con las condiciones de la regla. Tras esta evaluación inicial, AWS Config continúa realizando evaluaciones cada vez que se activa una. Los desencadenadores de evaluaciones están definidos como parte de la regla, y pueden incluir los siguientes tipos.

Tipo de desencadenador	Descripción
Cambios de configuración	AWS Config ejecuta las evaluaciones de la regla cuando hay un recurso que coincide con el alcance de la regla y se produce un cambio en la configuración del recurso. La evaluación se ejecuta después de AWS Config enviar una notificación de cambio de elemento de configuración.

Tipo de desencadenador	Descripción
	Usted elige qué recursos activan la evaluación al definir el ámbito de la regla. El ámbito puede incluir lo siguiente: • Uno o varios tipos de recursos • Una combinación de un tipo de recurso y un ID de recurso • Una combinación de una clave de etiqueta y un valor • Cuando se crea, se actualiza o se elimina cualquier recurso registrado AWS Config ejecuta la evaluación cuando detecta un cambio en un recurso que coincide con el alcance de la regla. Puede utilizar el ámbito para definir los recursos que activan evaluaciones.
Periódico	AWS Config ejecuta las evaluaciones de la regla con la frecuencia que usted elija; por ejemplo, cada 24 horas.
Híbrido	Algunas reglas tienen cambios de configura ción y desencadenadores periódicos. Para estas reglas, AWS Config evalúa sus recursos cuando detecta un cambio de configuración y también con la frecuencia que especifique.

Modos de evaluación

Hay dos modos de evaluación de las AWS Config reglas.

Modo de evaluación	Descripción
Proactiva	Utilice una evaluación proactiva para evaluar los recursos antes de que se implementen. Esto le permite evaluar si un conjunto de propiedades de un recurso, si se utiliza para definir un AWS recurso, cumple o no lo cumple, dado el conjunto de reglas proactivas que tiene en su cuenta en su región. Para obtener más información, consulte Modos de evaluación. Para obtener una lista de las reglas administradas que admiten la evaluació n proactiva, consulte la Lista de reglas AWS Config administradas por modo de evaluación.
Detective	Utilice la evaluación de detectives para evaluar los recursos que ya se han implementado. Esto le permite evaluar los ajustes de configuración de los recursos existentes.

> **Note**
>
> Las reglas proactivas no corrigen los recursos que están marcados como NON_COMPLIANT ni impiden su implementación.

Paquetes de conformidad

Un paquete de conformidad es un conjunto de AWS Config reglas y medidas correctivas que se pueden implementar fácilmente como una sola entidad en una cuenta y una región o en toda la organización. AWS Organizations

Los paquetes de conformidad se crean generando una plantilla YAML que contiene la lista de reglas administradas o personalizadas y las acciones de corrección de AWS Config . Puede implementar la plantilla utilizando la consola de AWS Config o la AWS CLI.

Para empezar rápidamente y evaluar su AWS entorno, utilice uno de los ejemplos de plantillas de paquetes de conformidad. También puede crear un archivo YAML del paquete de conformidad desde cero basándose en el paquete de conformidad personalizado. Un paquete de conformidad personalizado es un conjunto único de AWS Config reglas y acciones correctivas que puede implementar de forma conjunta en una cuenta y una AWS región, o en una organización. AWS Organizations

Las comprobaciones de procesos son un tipo de AWS Config regla que te permite realizar un seguimiento de las tareas externas e internas que requieren verificación como parte de los paquetes de conformidad. Estas comprobaciones se pueden agregar a un paquete de conformidad existente o a un paquete de conformidad nuevo. Puede realizar un seguimiento de todo el cumplimiento, incluidas las AWS Config duraciones y las comprobaciones manuales, en un solo lugar.

Acumulación de datos de varias cuentas y regiones

La agregación de datos multicuenta y multirregión AWS Config le permite agregar datos de AWS Config configuración y cumplimiento de varias cuentas y regiones en una sola cuenta. La agregación de datos multicuenta y multirregión es útil para que los administradores de TI centrales supervisen el cumplimiento de varias Cuentas de AWS cuentas de la empresa. El uso de agregadores no implica ningún costo adicional.

Cuenta de origen

Una cuenta de origen es la cuenta Cuenta de AWS desde la que desea agregar los datos de conformidad y configuración de los AWS Config recursos. Una cuenta de origen puede ser una cuenta individual o una organización de AWS Organizations. Puede proporcionar las cuentas de origen de forma individual o puede recuperarlas a través de ellas AWS Organizations.

Región de origen

Una región de origen es la AWS región desde la que desea agregar los datos AWS Config de configuración y conformidad.

Agregador

Un agregador recopila datos AWS Config de configuración y conformidad de varias regiones y cuentas de origen. Cree un agregador en la región en la que desee ver los datos agregados de AWS Config configuración y conformidad.

> **Note**
>
> Los agregadores proporcionan una vista de solo lectura de las cuentas y regiones de origen que el agregador está autorizado a ver; para ello, replican los datos de las cuentas de origen en la cuenta del agregador. Los agregadores no proporcionan acceso mutante ni a la cuenta ni a la región de origen. Por ejemplo, esto significa que no puede implementar reglas a través de un agregador ni enviar archivos de instantáneas a una cuenta o región de origen a través de un agregador.

Agregador vinculado a servicios

Un agregador vinculado a un servicio está vinculado a un agregador específico. Servicio de AWS El servicio vinculado establece los datos de configuración y cumplimiento en el ámbito.

Cuenta de agregador

Una cuenta de agregador es la cuenta en la que se crea un agregador.

Autorización

Como propietario de una cuenta de origen, la autorización se refiere a los permisos que concedes a una cuenta y región de un agregador para recopilar tus datos de AWS Config configuración y cumplimiento. La autorización no es necesaria si se agregan cuentas de origen que forman parte de AWS Organizations.

AWS Integraciones de servicios con AWS Config

AWS Config admite integraciones con varios otros AWS servicios. Esta lista no es exhaustiva.

AWS Organizations

Puede utilizarlas AWS Organizations para definir las cuentas que se utilizarán para la capacidad AWS Config de agregación de datos multicuenta y multirregión.AWS Organizations es un servicio de administración de cuentas que le ayuda a consolidar varias cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada. Al proporcionar sus AWS Organizations datos, puede supervisar el estado de cumplimiento en toda su organización. Para

obtener más información, consulte AWS Config and AWS Organizations en la Guía del usuario de AWS Organizations.

AWS Control Tower

AWS Control Tower se activa AWS Config en todas las cuentas inscritas, de modo que puede supervisar el cumplimiento mediante controles de detección, registrar los cambios en los recursos y entregar los registros de cambios en los recursos a la cuenta de archivo de registros. Para obtener más información, consulte Monitor resource changes with AWS Config en la Guía del usuario de AWS Control Tower.

AWS CloudTrail

AWS Config se integra con AWS CloudTrail para correlacionar los cambios de configuración con eventos particulares de su cuenta. Puede utilizar los CloudTrail registros para obtener los detalles del evento que provocó el cambio, como quién realizó la solicitud, a qué hora y desde qué dirección IP. Puedes navegar a la AWS Config cronología desde la CloudTrail consola para ver los cambios de configuración relacionados con las actividades de tu AWS API.

Para obtener más información, consulte Registrar las llamadas a la AWS Config API AWS CloudTrail en la Guía para AWS Config desarrolladores y Crear un banco de datos de eventos para los elementos de AWS Config configuración con la consola en la Guía del AWS CloudTrail usuario.

AWS Security Hub CSPM

AWS Security Hub CSPM centraliza los controles de seguridad de otros AWS servicios, incluidas las AWS Config reglas. Security Hub habilita y controla las reglas de AWS Config para verificar que las configuraciones de los recursos encajen con las prácticas recomendadas.AWS Config Actívela en todas las cuentas de todas las regiones en las que Security Hub CSPM ejecute comprobaciones de seguridad en los recursos de su entorno. Para obtener más información, consulte AWS services that send findings to Security Hub en la Guía del usuario de AWS Security Hub CSPM.

> **Algunas reglas relacionadas con el CSPM de Security Hub son periódicas y no dependen de los elementos de configuración**
>
> Algunas reglas relacionadas con el CSPM de Security Hub son periódicas. Estas reglas se ejecutan sin que el registrador de configuración esté habilitado y no dependen de elementos de configuración (CI).

Esto significa que si ve la página de reglas, no aparece ningún CI ni recurso compatible en la lista. Si selecciona el ID del recurso, aparecerá el siguiente error: `The provided resource ID and resource type cannot be found`. Este es el comportamiento esperado.

AWS Trusted Advisor

AWS Config Las reglas gestionadas impulsan un conjunto de Trusted Advisor comprobaciones en todas las categorías. Al activar determinadas reglas gestionadas, las Trusted Advisor comprobaciones correspondientes se activan automáticamente. Para ver quéTrusted Advisor comprobaciones se basan en reglas AWS Config gestionadas específicas, consulta la referencia sobre AWS Trusted Advisor comprobaciones en la Guía del AWS Support usuario.

Los cheques AWS Config automatizados están disponibles para los clientes con los planes AWS Business Support, AWS Enterprise On-Ramp y AWS Enterprise Support. Si habilita uno de estos planes AWS Support AWS Config y lo tiene, verá automáticamente las recomendaciones basadas en las correspondientes reglas AWS Config gestionadas implementadas.

No se permiten las solicitudes de actualización y no se pueden excluir los recursos

Los resultados de estas comprobaciones se actualizan automáticamente en función de las actualizaciones de las reglas gestionadas provocadas por cambios.AWS Config No se permiten las solicitudes de actualización. Actualmente, no se pueden excluir recursos de estas comprobaciones.

Para obtener más información, consulte Ver las Trusted Advisor comprobaciones impulsadas por AWS Config en la Guía del AWS Support usuario.

AWS Audit Manager

Puede usar Audit Manager para capturar AWS Config las evaluaciones como evidencia para las auditorías. Al crear o editar un control personalizado, puede especificar una o más AWS Config reglas como mapeo de fuentes de datos para la recopilación de pruebas.AWS Config realiza comprobaciones de conformidad en función de estas reglas, y Audit Manager informa de los resultados como evidencia de las comprobaciones de conformidad. Para obtener más información,

consulte AWS Config Rules supported by AWS Audit Manager en la Guía del usuario de AWS Audit Manager.

AWS Systems Manager

AWS Config se integra con Systems Manager para registrar los cambios de configuración del software en sus EC2 instancias y servidores de Amazon en su entorno local. Con esta integración, puede obtener visibilidad de las configuraciones del sistema operativo (SO), las actualizaciones a nivel del sistema, las aplicaciones instaladas, la configuración de la red y mucho más.AWS Config también proporciona un historial de los cambios en la configuración del sistema operativo y del sistema, junto con los cambios en la configuración de la infraestructura registrados en las instancias de Amazon EC2 . Puede navegar a la AWS Config cronología desde la consola de Systems Manager para ver los cambios de configuración de las EC2 instancias gestionadas de Amazon. Puede utilizarlo AWS Config para ver el historial de inventario de Systems Manager y realizar un seguimiento de los cambios de todas las instancias gestionadas.

Para obtener más información, consulte Integración con AWS los servicios | Administración y gobierno, implementación AWS Config del registrador de configuración y del paquete de AWS Config conformidad en la Guía del AWS Systems Manager usuario.

AWS Firewall Manager

Para usar el Firewall Manager, debe habilitarlo AWS Config para cada una de sus cuentas de AWS Organizations miembro. Cuando se crean nuevas aplicaciones, Firewall Manager es el único servicio para crear reglas de firewall y políticas de seguridad, así como para aplicarlas de manera uniforme. Para obtener más información, consulte Habilitar AWS Config en la AWS WAF guía para AWS Shield Advanced desarrolladores y en la Guía para desarrolladores.AWS Firewall Manager

> **Note**
>
> Firewall Manager depende del registro continuo para supervisar los recursos. Si utiliza Firewall Manager, se recomienda configurar la frecuencia de registro en Continua. Para obtener más información sobre el registro continuo y diario, consulte Recording Frequency.

Hosts EC2 dedicados de Amazon

AWS Config se integra con Amazon EC2 Dedicated Hosts para evaluar el cumplimiento de las licencias.AWS Config registra cuándo se lanzan, se detienen o se cierran las instancias en un host

dedicado y combina esta información con la información a nivel de host e instancia relevante para las licencias de software, como el ID de host, la imagen de Amazon Machine (AMI) IDs, el número de sockets y los núcleos físicos. Esto le ayuda a AWS Config utilizarlos como fuente de datos para sus informes sobre licencias. Puede navegar a la AWS Config cronología desde la consola de Amazon EC2 Dedicated Hosts para ver los cambios de configuración de sus hosts EC2 dedicados de Amazon.

Para obtener más información, consulte Realice el seguimiento de los cambios, en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux, o Realice el seguimiento de los cambios, en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Windows.

Equilibrador de carga de aplicación

AWS Config se integra con el servicio Elastic Load Balancing (ELB) para registrar los cambios de configuración en los balanceadores de carga de aplicaciones.AWS Config también incluye las relaciones con los grupos EC2 de seguridad y subredes de Amazon asociados. VPCs Puede usar esta información para el análisis de la seguridad y para la resolución de problemas. Por ejemplo, puede comprobar qué grupos de seguridad están asociados a su equilibrador de carga de aplicación en cualquier momento. Puede navegar hasta la AWS Config cronología desde la consola ELB para ver los cambios de configuración de sus balanceadores de carga de aplicaciones.

AWS CodeBuild

AWS Config proporciona un inventario de sus AWS recursos y un historial de los cambios de configuración de estos recursos.AWS Config admite AWS CodeBuild; como AWS recurso, lo que significa que el servicio puede realizar un seguimiento de sus CodeBuild proyectos. Para obtener más información, consulte Uso AWS Config con CodeBuild ejemplos en la Guía del AWS CodeBuild usuario.

AWS X-Ray

AWS X-Ray se integra AWS Config para registrar los cambios de configuración realizados en sus recursos de cifrado de X-Ray. Puede utilizarlos AWS Config para inventariar los recursos de cifrado de X-Ray, auditar el historial de configuración de X-Ray y enviar notificaciones en función de los cambios en los recursos. Para obtener más información, consulte Tracking X-Ray encryption configuration changes with AWS Config en la Guía del desarrollador de AWS X-Ray.

AWS Service Management Connector

The AWS Service Management Connector for ServiceNow puede sincronizar AWS Config datos de varias cuentas y regiones mediante un agregador. Para obtener más información, consulte Integración AWS Config ServiceNow en la Guía del AWS Service Management Connector administrador.

Amazon API Gateway

Puedes usarlo AWS Config para registrar los cambios de configuración realizados en tus recursos de API de API Gateway y enviar notificaciones en función de los cambios en los recursos. Mantener un historial de los cambios de configuración de los recursos de API Gateway es útil para los casos de uso relacionados con la solución de problemas operativos, auditoría y conformidad. Para obtener más información, consulte Monitoreo de la configuración de la API de API Gateway con AWS Config en la Guía para desarrolladores de API Gateway.

Region Support para AWS Config

Consideraciones

Algunas funciones de solo AWS Config se admiten en un subconjunto de AWS las regiones en las que AWS Config se admiten.

Administración de recursos

- Para ver una lista de los tipos de AWS recursos compatibles en qué regiones, consulte Cobertura de recursos por disponibilidad regional.

AWS Config Reglas

- Para ver una lista de AWS Config las reglas que se admiten en cada región, consulte la Lista de reglas AWS Config administradas por disponibilidad regional.
- Para ver una lista de las regiones que admiten el despliegue de AWS Config reglas a nivel organizacional, consulta Organizational Rules | Region Support.

Paquetes de conformidad

- Para obtener una lista de las regiones que admiten paquetes de conformidad y la implementación organizativa de los paquetes de conformidad, consulte Paquetes de conformidad | Compatibilidad de la región.

Corrección

- Para obtener una lista de las regiones que apoyan las acciones de remediación de las AWS Config normas, consulte Remediation Actions | Region Support.

Agregadores

- Para obtener una lista de las regiones que admiten los agregadores, consulte Agregadores | Compatibilidad de la región.

Consultas avanzadas

- Para obtener una lista de las regiones que admiten consultas avanzadas, consulte Consultas avanzadas | Compatibilidad de la región.
- Para obtener una lista de las regiones que admiten el procesador de consultas en lenguaje natural para consultas avanzadas, consulte Procesador de consultas en lenguaje natural para consultas avanzadas | Compatibilidad de la región.

Lista de regiones compatibles

En la siguiente tabla se enumeran las AWS regiones en las que puede activarlas. AWS Config

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
Este de EE. UU.	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
(Norte de Virginia)			
Oeste de EE. UU. (Norte de California)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Tailandia)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
México (centro)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Límites de los servicios para AWS Config

En la siguiente tabla se describen los límites de AWS Config. A menos que se indique lo contrario, las cuotas se pueden aumentar previa solicitud. Puede solicitar un aumento de cuota.

Para obtener información acerca de otros límites en AWS, consulte Límites de los servicios de AWS.

Etiquetas de recursos

Descripción	Valor limitado	Se puede aumentar
Número máximo de etiquetas por recurso	50	No

AWS ConfigReglas de

Descripción	Valor limitado	Se puede aumentar
Número máximo de reglas de AWS Config por región y cuenta	1 000	No

Paquetes de conformidad de cuenta única

Descripción	Valor limitado	Se puede aumentar
Número máximo de paquetes de conformidad por cuenta	50	No
Número máximo de reglas de AWS Config por paquete de conformidad	130	No

> **Note**
>
> Las reglas de AWS Config en los paquetes de conformidad se incluyen en el límite del número máximo de reglas de AWS Config por región y cuenta.

Paquetes de conformidad de la organización

Descripción	Valor limitado	Se puede aumentar
Número máximo de paquetes de conformidad por organización	50	No
Número máximo de reglas de AWS Config por paquete de conformidad de la organización	130	No

> **Note**
>
> La implementación en el nivel de la organización cuenta como límite en el caso de las cuentas secundarias. Las reglas de AWS Config en los paquetes de conformidad se incluyen en el límite del número máximo de reglas de AWS Config por región y cuenta.

Agregadores

Descripción	Valor limitado	Se puede aumentar
Número máximo de agregadores de configuración	50	Sí
Número máximo de cuentas en un agregador	10000	No
Número máximo de cuentas agregadas o eliminadas por semana para todos los agregadores	1 000	Sí

> **Note**
>
> Tanto los agregadores en el nivel de organización como los agregadores de cuentas individuales se incluyen en el recuento del límite para el número máximo de agregadores de configuración.

Consultas avanzadas

Descripción	Valor limitado	Se puede aumentar
Número máximo de consultas guardadas en una sola cuenta y una región	300	Sí

Información complementaria y recursos relacionados para AWS Config

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con este servicio.

- AWS Config – página web principal con información sobre AWS Config.
- AWS Config Precios de
- Preguntas frecuentes técnicas de
- Kit de desarrollo de reglas (RDK) de AWS Config: herramienta de código abierto que le ayuda a configurar AWS Config, crear reglas y probarlas con una variedad de tipos de recursos de AWS.
- Socios: enlaces a productos de socios que se integran completamente con AWS Config para ayudarle a visualizar, monitorizar y administrar los datos desde la configuración de flujo, las instantáneas de configuración o el historial de configuración.
- Clases y talleres: enlaces a cursos basados en roles y especializados, además de laboratorios autoguiados para ayudarlo a desarrollar sus conocimientos sobre AWS y obtener experiencia práctica.
- Centro para desarrolladores de AWS: explore los tutoriales, descargue herramientas y obtenga información sobre los eventos para desarrolladores de AWS.

- Herramientas para desarrolladores de AWS: enlaces a herramientas para desarrolladores, SDK, conjuntos de herramientas de IDE y herramientas de línea de comandos para desarrollar y administrar aplicaciones de AWS.
- Centro de recursos de introducción: aprenda a configurar su Cuenta de AWS, únase a la comunidad de AWS y lance su primera aplicación.
- Tutoriales prácticos: comience con tutoriales paso a paso antes de lanzar su primera aplicación en AWS.
- Documentos técnicos de AWS: enlaces a una lista completa de documentos técnicos de AWS que tratan una gran variedad de temas técnicos, como arquitecturas, seguridad y economía de la nube, escritos por arquitectos de soluciones de AWS o expertos técnicos.
- Centro de AWS Support: punto central para crear y administrar los casos de AWS Support. También incluye enlaces a otros recursos útiles como foros, preguntas técnicas frecuentes, estado de los servicios y de AWS Trusted Advisor.
- Soporte: la página web principal para obtener información acerca de Soporte, un canal de soporte individualizado y de respuesta rápida que le ayudará a crear y ejecutar aplicaciones en la nube.
- Contacta con nosotros – Un punto central de contacto para las consultas relacionadas con la facturación AWS, cuentas, eventos, abuso y demás problemas.
- AWSTérminos del sitio de : información detallada sobre nuestros derechos de autor y marca comercial, su cuenta, licencia y acceso al sitio, entre otros temas.

AWS Kits de desarrollo de software para AWS Config

Un kit de desarrollo de software (SDK) de AWS facilita la creación de aplicaciones que obtienen acceso a servicios de infraestructura de AWS rentables, escalables y de confianza. Con los SDK de AWS, puede ponerse en marcha en cuestión de minutos con un único paquete descargable que incluye la biblioteca, ejemplos de código y documentación de referencia. En la siguiente tabla, se muestran los SDK y las bibliotecas de terceros disponibles que puede utilizar para obtener acceso a AWS Config mediante programación.

Tipo de acceso	Descripción
AWS SDK	AWS ofrece los siguientes SDK: • AWS Documentación del SDK para C++ de • AWS Mobile SDK for iOS Documentación de

Tipo de acceso	Descripción
	• AWS Documentación del SDK para Go de • AWS SDK para Java Documentación de • AWS Documentación del SDK para JavaScript de • AWS SDK para .NET Documentación de • AWS SDK para PHP Documentación de • AWS SDK para Python (Boto) Documentación de • AWS SDK para Ruby Documentación de
Bibliotecas de terceros	Los desarrolladores de la comunidad de desarrolladores de AWS también proporcionan sus propias bibliotecas, que puede encontrar en los siguientes centros de desarrolladores de AWS: • AWS Centro de desarrolladores de Java de • AWS Centro de desarrolladores de JavaScript de • AWS Centro de desarrolladores de PHP de • AWS Centro de desarrolladores de Python de • AWS Centro de desarrolladores de Ruby de • AWS Centro de desarrolladores de Windows y .NET de

Cómo empezar con AWS Config

AWS Config proporciona una vista detallada de la configuración de AWS los recursos de su Cuenta de AWS. Con él AWS Config, puede revisar los cambios en las configuraciones y las relaciones entre AWS los recursos, explorar el historial de configuración de los recursos y utilizar las reglas para determinar el cumplimiento. Para obtener más información, consulte ¿Qué es AWS Config? y Cómo AWS Config funciona.

Registrarse en AWS

Temas

- Inscríbase en una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWSAWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión Consola de administración de AWScomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In.

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center.

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center.

Formas de empezar AWS Config

Después de suscribirse a una Cuenta de AWS, puede empezar AWS Config con la Consola de administración de AWSAWS CLI o la AWS SDKs.

- Configuración AWS Config con la consola
- Configuración AWS Config con el AWS CLI
- Uso AWS Config del servicio con el AWS SDK

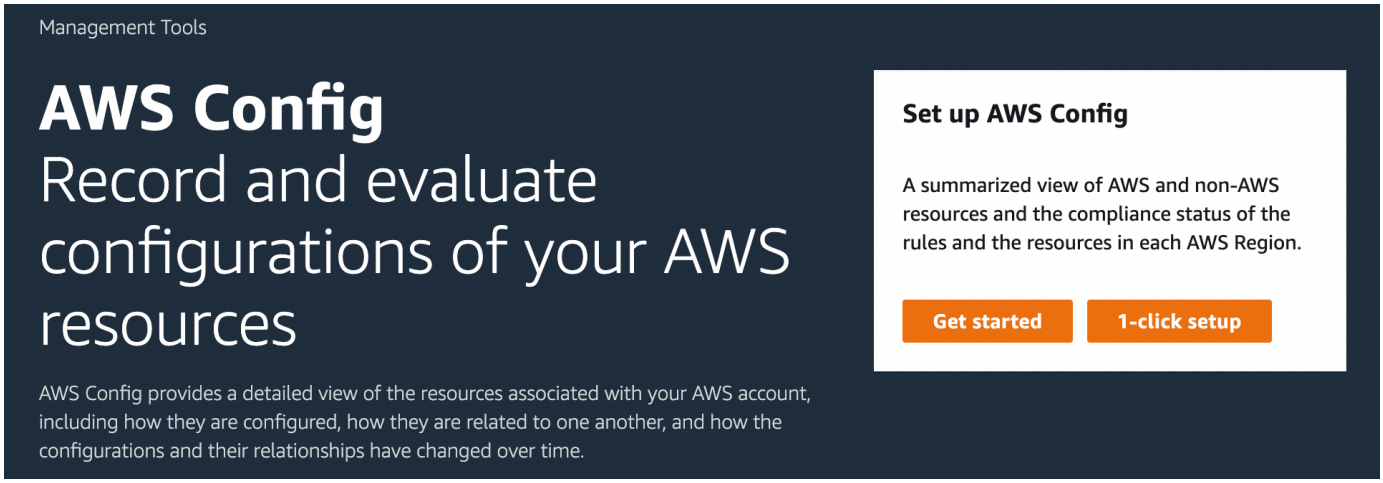
Configuración de AWS Config con la consola

La Consola de administración de AWS proporciona un proceso de configuración rápido y simplificado para configurar AWS Config.

Configuración

Para configurar AWS Config con la consola

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Config en https://console.aws.amazon.com/config/home.
2. Si es la primera vez que se abre la consola de AWS Config o que configura AWS Config en una nueva región, la página de la consola AWS Config tiene este aspecto:



3. Elija la configuración en un clic para iniciar AWS Config según las prácticas recomendadas de AWS. También puede elegir Introducción para seguir un proceso de configuración más detallado.

Temas

- Configuración con 1 clic para AWS Config
- Configuración manual para AWS Config

Configuración con 1 clic para AWS Config

AWS Config La configuración con un solo clic ayuda a simplificar el proceso de inicio para los clientes de AWS Config consolas al reducir el número de selecciones manuales. Para ver todas las selecciones manuales del proceso de configuración, consulte Manual setup.

Para configurarlo AWS Config con la consola mediante la configuración con un solo clic

1. Inicia sesión en la AWS Config consola Consola de administración de AWS y ábrela en https://console.aws.amazon.com/config/casa.
2. Seleccione configuración en un clic.

La página de configuración incluye tres pasos, pero mediante el flujo de trabajo de configuración en un clic, se le redirige automáticamente al paso 3 (revisión). A continuación, se describe el procedimiento con detalle.

- Configuración: para seleccionar la forma en que la AWS Config consola registra los recursos y las funciones, y elegir dónde se envían el historial de configuración y los archivos de instantáneas de la configuración.
- Reglas: Para Regiones de AWS que AWS Config las reglas sean compatibles, este paso le permite configurar las reglas administradas iniciales que puede agregar a su cuenta. Tras la configuración, AWS Config evaluará sus AWS recursos en función de las reglas que haya elegido. Después de configurar, podrá crear reglas adicionales y actualizar las existentes en su cuenta.
- Revisión: para verificar los detalles de configuración.

Paso 1: configuración

Estrategia de registro

La opción de registrar todos los tipos de recursos con anulaciones personalizables está seleccionada para usted. AWS Config registrará todos los tipos de recursos compatibles actuales y futuros en esta región. Para obtener más información, consulte Tipos de recursos admitidos.

- Configuración predeterminada

  La frecuencia de registro predeterminada está configurada en Continua para usted. Esto significa que AWS Config registra los cambios de configuración de forma continua cada vez que se produce un cambio.

  AWS Config también admite la opción de configurar la frecuencia de grabación en Diaria. Si selecciona esta opciíon después de la configuración, recibirá un elemento de configuración (CI) que representa el estado más reciente de sus recursos durante el último período de 24 horas, solo si es diferente del CI anterior registrado. Para obtener más información, consulte Frecuencia de registro.

  > **Note**
  >
  > AWS Firewall Manager depende de la grabación continua para monitorear sus recursos. Si utiliza Firewall Manager, se recomienda configurar la frecuencia de registro en Continua.

- Anular la configuración: opcional

  También puede anular la frecuencia de registro para tipos de recursos específicos o excluir tipos de recursos específicos del registro. Para anular la configuración predeterminada, selecciona

Configuración en el panel de navegación izquierdo de la AWS Config consola y, a continuación, selecciona Editar.

Consideraciones al registrar los recursos

Número elevado de evaluaciones AWS Config

Es posible que notes un aumento de la actividad en tu cuenta durante el primer mes de grabación con AWS Config en comparación con los meses siguientes. Durante el proceso de arranque inicial, AWS Config realiza evaluaciones de todos los recursos de tu cuenta que hayas seleccionado para AWS Config registrarlos.

Si ejecuta cargas de trabajo efímeras, es posible que vea un aumento de la actividad de AWS Config debido a que registra los cambios de configuración asociados con la creación y la eliminación de estos recursos temporales. Una carga de trabajo efímera es el uso temporal de recursos informáticos que se cargan y ejecutan cuando es necesario. Los ejemplos incluyen instancias de spot de Amazon Elastic Compute Cloud (Amazon EC2), trabajos de Amazon EMR y AWS Auto Scaling. Si quiere evitar el aumento de actividad derivado de la ejecución de cargas de trabajo efímeras, puede configurar el registrador de configuraciones de modo que excluya estos tipos de recursos de la grabación, o puede ejecutar estos tipos de cargas de trabajo en una cuenta independiente con la opción AWS Config desactivada para evitar aumentar el registro de la configuración y las evaluaciones de las reglas.

Tipos de recursos globales | Los clústeres globales de Aurora se incluyen inicialmente en la grabación

El tipo `AWS::RDS::GlobalCluster` de recurso se registrará en todas las AWS Config regiones compatibles en las que esté activado el registrador de configuración.

Si no desea registrar `AWS::RDS::GlobalCluster` en todas las regiones habilitadas, puede excluir este tipo de recurso de la grabación después de la configuración. En la barra de navegación izquierda, elija Configuración y, después, Editar. Desde Editar, vaya a Configuración de anulación en la sección Método de registro, elija `AWS::RDS::GlobalCluster` y, a continuación, la opción de anulación “Excluir del registro”.

Tipos de recursos globales | Los tipos de recursos de IAM se excluyen inicialmente del registro

Inicialmente, se excluyen del registro «todos los tipos de recursos de IAM registrados globalmente» para ayudarle a reducir los costes. Esta agrupación incluye usuarios, grupos, roles y políticas

administradas por el cliente de de IAM. Seleccione Eliminar para eliminar la anulación e incluir estos recursos en el registro.

Además, estos tipos de recursos de IAM globales (`AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role` y `AWS::IAM::Policy`) no se pueden registrar en las regiones admitidas por AWS Config después de febrero de 2022. Para obtener una lista de esas regiones, consulte AWS Recursos de grabación | Recursos globales.

Gobernanza de datos

En esta sección, selecciona el período de retención de AWS Config datos predeterminado para conservar los datos durante 7 años (2557 días).

La opción Utilizar una función AWS Config vinculada a un servicio existente está seleccionada automáticamente y configurada para esa función.AWS Config Los roles vinculados al servicio están predefinidos AWS Config e incluyen todos los permisos que el servicio requiere para llamar a otros servicios. AWS

Modo de entrega

En esta sección, la opción Elegir un bucket de su cuenta se selecciona en su nombre. De forma predeterminada, esta selección se aplicará al bucket de la cuenta cuyo nombre tenga el formato `config-bucket-`*`accountid`*. Por ejemplo, `config-bucket-012345678901`. Si no ha creado ningún bucket con ese formato, se creará uno. Para crear un bucket, consulte Crear un bucket en la Guía del usuario de Amazon Simple Storage Service.

Para obtener más información acerca los buckets de S3, consulte Descripción general de los buckets en la Guía del usuario de Amazon Simple Storage Service.

Paso 2: reglas

En Reglas administradas por AWS , no se seleccionará ninguna regla para usted en este paso. En su lugar, le recomendamos que cree y actualice las reglas una vez que haya terminado de configurar la cuenta.

Paso 3: revisión

Revisa los detalles de la AWS Config configuración. Puede volver a editar los cambios de cada sección. Selecciona Confirmar para finalizar la configuración AWS Config.

Configuración manual para AWS Config

Con el flujo de trabajo de introducción, puede realizar todas las selecciones manuales del proceso de configuración para empezar a utilizar la AWS Config consola. Si dese informarse sobre un proceso de inicio simplificado, consulte Configuración en un clic.

Para configurarla AWS Config con la consola mediante Get Started

1. Inicia sesión en la AWS Config consola Consola de administración de AWS y ábrela en https://console.aws.amazon.com/config/casa.
2. Elija Comenzar.

La página de configuración incluye tres pasos. A continuación, se proporciona un desglose del procedimiento después de seleccionar Introducción.

- Configuración: para seleccionar la forma en que la AWS Config consola registra los recursos y las funciones, y elegir dónde se envían el historial de configuración y los archivos de instantáneas de la configuración.
- Reglas: Para Regiones de AWS que AWS Config las reglas sean compatibles, este paso le permite configurar las reglas administradas iniciales que puede agregar a su cuenta. Tras la configuración, AWS Config evaluará sus AWS recursos en función de las reglas que haya elegido. Después de configurar, podrá crear reglas adicionales y actualizar las existentes en su cuenta.
- Revisión: para verificar los detalles de configuración.

Paso 1: configuración

Estrategia de registro

En la sección Método de grabación, elija una estrategia de registro. Puede especificar los AWS recursos que AWS Config desea registrar.

All resource types with customizable overrides

> Se configura AWS Config para registrar los cambios de configuración de todos los tipos de recursos compatibles actuales y futuros en esta región. Puede anular la frecuencia de registro para tipos de recursos específicos o excluir tipos de recursos específicos del registro. Para obtener más información, consulte Tipos de recursos admitidos.

- Configuración predeterminada

  Configure la frecuencia de registro predeterminada para todos los tipos de recursos compatibles actuales y futuros. Para obtener más información, consulte Frecuencia de registro.

  - Grabación continua: AWS Config registrará los cambios de configuración de forma continua siempre que se produzca un cambio.
  - Registro diario: recibirá un elemento de configuración (CI) que representa el estado más reciente de sus recursos durante el último período de 24 horas, solo si es diferente del CI anterior registrado.

  > **Note**
  >
  > AWS Firewall Manager depende de la grabación continua para monitorear sus recursos. Si utiliza Firewall Manager, se recomienda configurar la frecuencia de registro en Continua.

- Anular la configuración

  Puede anular la frecuencia de registro para tipos de recursos específicos o excluir tipos de recursos específicos del registro. Si cambia la frecuencia de registro de un tipo de recurso, o deja de registrar un tipo de recurso, los elementos de configuración que ya estaban registrados permanecerán sin cambios.

Specific resource types

Se configura AWS Config para registrar los cambios de configuración solo para los tipos de recursos que especifique.

- Tipos de recurso específicos

  Elija un tipo de recurso que desee registrar y su frecuencia. Para obtener más información, consulte Frecuencia de registro.

  - Grabación continua: AWS Config registrará los cambios de configuración de forma continua siempre que se produzca un cambio.
  - Registro diario: recibirá un elemento de configuración (CI) que representa el estado más reciente de sus recursos durante el último período de 24 horas, solo si es diferente del CI anterior registrado.

> **Note**
>
> AWS Firewall Manager depende de la grabación continua para monitorear sus recursos. Si utiliza Firewall Manager, se recomienda configurar la frecuencia de registro en Continua.

Si cambia la frecuencia de registro de un tipo de recurso, o deja de registrar un tipo de recurso, los elementos de configuración que ya estaban registrados permanecerán sin cambios.

Consideraciones al registrar los recursos

Alto número de AWS Config evaluaciones

Es posible que notes un aumento de la actividad en tu cuenta durante el primer mes de grabación con AWS Config en comparación con los meses siguientes. Durante el proceso de arranque inicial, AWS Config realiza evaluaciones de todos los recursos de tu cuenta que hayas seleccionado para AWS Config registrarlos.

Si ejecuta cargas de trabajo efímeras, es posible que vea un aumento de la actividad de AWS Config debido a que registra los cambios de configuración asociados con la creación y la eliminación de estos recursos temporales. Una carga de trabajo efímera es el uso temporal de recursos informáticos que se cargan y ejecutan cuando es necesario. Algunos ejemplos son las instancias puntuales de Amazon Elastic Compute Cloud (Amazon EC2), los trabajos de Amazon EMR y. AWS Auto Scaling Si quiere evitar el aumento de actividad derivado de la ejecución de cargas de trabajo efímeras, puede configurar el registrador de configuraciones de modo que excluya estos tipos de recursos de la grabación, o puede ejecutar estos tipos de cargas de trabajo en una cuenta independiente con la opción AWS Config desactivada para evitar aumentar el registro de la configuración y las evaluaciones de las reglas.

Considerations: All resource types with customizable overrides

Tipos de recursos registrados de forma global | Los clústeres globales de Aurora se incluyen inicialmente en el registro

El tipo `AWS::RDS::GlobalCluster` de recurso se registrará en todas las AWS Config regiones compatibles en las que el registrador de configuración esté habilitado.

Si no desea registrar `AWS::RDS::GlobalCluster` en todas las regiones habilitadas, elija «AWS RDS GlobalCluster» y «Excluir del registro».

Tipos de recursos globales | Los tipos de recursos de IAM se excluyen inicialmente del registro

Inicialmente, se excluyen del registro los tipos de recursos de IAM globales, para ayudarle a reducir los costos. Esta agrupación incluye usuarios, grupos, roles y políticas administradas por el cliente de de IAM. Seleccione Eliminar para eliminar la anulación e incluir estos recursos en el registro.

Además, los tipos de recursos de IAM globales (`AWS::IAM::User`, `AWS::IAM::GroupAWS::IAM::Role`, y`AWS::IAM::Policy`) no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para obtener una lista de esas regiones, consulte AWS Recursos de grabación | Recursos globales.

Límites

Puede añadir hasta 100 anulaciones de frecuencia y 600 anulaciones de exclusión.

No se puede especificar el registro diario para los siguientes tipos de recursos:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

Disponibilidad por región

Antes de especificar el tipo de recurso AWS Config que deseas rastrear, comprueba la cobertura de recursos por región y disponibilidad para ver si el tipo de recurso es compatible con la AWS región en la que lo configuraste AWS Config. Si al menos una región admite un tipo de recurso, puede habilitar el registro de ese tipo de recurso en todas las regiones admitidas AWS Config, incluso si el tipo de recurso especificado no es compatible con la AWS región en la que lo configuró AWS Config. AWS Config

Límites

No hay límites si todos los tipos de recursos tienen la misma frecuencia. Puede agregar hasta 100 tipos de recursos con la frecuencia diaria si al menos un tipo de recursos está configurado como Continuo.

No se admite el registro diario para los siguientes tipos de recursos:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Gobernanza de datos

- Para el período de retención de datos, elija el período de retención predeterminado para conservar AWS Config los datos durante 7 años (2557) o establezca un período de retención personalizado para los artículos registrados por. AWS Config

  AWS Config le permite eliminar sus datos especificando un período de retención para usted. `ConfigurationItems` Cuando se especifica un periodo de retención, AWS Config conserva su `ConfigurationItems` para ese periodo especificado. Puede elegir un período entre un mínimo de 30 días y un máximo de 7 años (2557 días). AWS Config elimina los datos anteriores al período de retención especificado.
- Para la función de IAM AWS Config, elija una función AWS Config vinculada al servicio existente o una función de IAM de su cuenta.
  - Los roles vinculados al servicio están predefinidos AWS Config e incluyen todos los permisos que el servicio requiere para llamar a otros servicios. AWS

    > **Note**
    >
    > Recomendación: Utilice el rol vinculado al servicio
    > Es recomendable que utilice el rol vinculado al servicio. Un rol vinculado a un servicio añade todos los permisos necesarios para que AWS Config se ejecute según lo esperado.
  - También puede elegir un rol de IAM entre uno de sus roles y políticas de permisos preexistentes

    > **Note**
    >
    > Políticas y resultados de cumplimiento
    > Las políticas de IAM y otras políticas gestionadas AWS Organizations pueden afectar a la disponibilidad de permisos para registrar los cambios de configuración de los recursos. AWS Config Además, las reglas evalúan directamente la configuración de un

recurso y no tienen en cuenta estas políticas al ejecutar las evaluaciones. Asegúrese de que las políticas en vigor se ajusten a la forma en que piensa utilizar AWS Config.
Mantenga el nivel de los permisos al mínimo al reutilizar un rol de IAM
Si utiliza un AWS servicio que utiliza AWS Config, como AWS Security Hub CSPM o AWS Control Tower, y ya se ha creado un rol de IAM, asegúrese de que el rol de IAM que utilice al configurar AWS Config mantenga los mismos permisos mínimos que el rol de IAM preexistente. Debe hacerlo para asegurarse de que el otro AWS servicio siga ejecutándose según lo previsto.
Por ejemplo, si AWS Control Tower tiene una función de IAM que AWS Config permite leer objetos de S3, asegúrese de conceder los mismos permisos a la función de IAM que utilizó al configurar. AWS Config De lo contrario, podría interferir con el funcionamiento de AWS Control Tower .

Modo de entrega

- Para Método de entrega, elija el bucket de S3 al que AWS Config envía archivos de historial de configuración y de instantáneas de configuración:
  - Crear un bucket: en Nombre del bucket de S3, escriba un nombre para el bucket de S3.

    El nombre que escriba debe ser único entre todos los nombres de buckets existentes en Amazon S3. Una forma de garantizar la exclusividad consiste en incluir un prefijo; por ejemplo, el nombre de su organización. No se puede cambiar el nombre del bucket después de crearlo. Para obtener más información, consulte Restricciones y limitaciones de los buckets en la Guía del usuario de Amazon Simple Storage Service.
  - Elegir un bucket de su cuenta: en Nombre del bucket de S3, elija el bucket que prefiera.
  - Elegir un bucket de otra cuenta: en Nombre del bucket de S3, escriba el nombre del bucket.

> **Note**
>
> Permisos de buckets
> Si eliges un bucket de otra cuenta, ese bucket debe tener políticas que le concedan permisos de acceso. AWS Config Para obtener más información, consulte Permisos del bucket de Amazon S3 para el canal AWS Config de entrega.

- Para el tema Amazon SNS, elija Transmitir los cambios de configuración y las notificaciones a un tema de Amazon SNS para AWS Config enviar notificaciones como la entrega del historial de configuración, la entrega de instantáneas de la configuración y el cumplimiento.
- Si ha elegido que la AWS Config transmisión se dirija a un tema de Amazon SNS, elija el tema de destino:
  - Crear un tema: en Nombre del tema, escriba un nombre para el tema de SNS.
  - Elegir un tema de su cuenta: en Nombre del tema, seleccione el tema que prefiera.
  - Elegir un tema de otra cuenta: en Nombre del tema, escriba el nombre de recurso de Amazon (ARN) del tema. Si eliges un tema de otra cuenta, el tema debe tener políticas que concedan permisos de acceso. AWS Config Para obtener más información, consulte Permisos para el tema de Amazon SNS.

> **Note**
>
> Región para el tema de Amazon SNS
> El tema Amazon SNS debe existir en la misma región que la región en la que lo configuró. AWS Config

Paso 2: reglas

Si se está configurando AWS Config en una región que admite reglas, seleccione Siguiente.

Paso 3: revisión

Revisa los detalles de la AWS Config configuración. Puede volver a editar los cambios de cada sección. Selecciona Confirmar para finalizar la configuración AWS Config.

Para obtener más información

Para obtener más información sobre cómo buscar los recursos existentes en su cuenta y comprender las configuraciones de sus recursos, consulte Looking up Resources, Viewing Compliance Informance y Viewing Compliance History.

También puede utilizar Amazon Simple Queue Service para supervisar AWS los recursos mediante programación. Para obtener más información, consulte Supervisión de los cambios en los AWS recursos con Amazon SQS.

Configuración de AWS Config con la AWS CLI

La AWS CLI es una herramienta unificada para administrar los servicios de AWS. Solo necesita descargar y configurar una herramienta para poder controlar varios servicios de AWS desde la línea de comandos y usar scripts para automatizarlos. Para obtener más información sobre la AWS CLI y para obtener instrucciones sobre la instalación de herramientas de la AWS CLI, consulte lo siguiente en la Guía del usuario de AWS Command Line Interface.

- AWS Command Line Interface Guía del usuario de
- Configuración inicial de la AWS Command Line Interface

Si es necesario, introduzca `aws configure` para definir que la AWS CLI utilice una región de AWS en la que haya AWS Config disponibles.

Configuración

Consulte los siguientes temas para configurar AWS Config con la AWS CLI.

Temas

- Requisitos previos para la configuración AWS Config con el AWS CLI
- Inicio de AWS Config con un registrador de configuración administrado por el cliente utilizando la AWS CLI
- Verificación de que AWS Config se ha iniciado correctamente con el AWS CLI

Requisitos previos para la configuración AWS Config con el AWS CLI

Antes de AWS configurarlo AWS CLI, debe crear un bucket de Amazon S3, un tema de Amazon SNS y un rol de IAM con políticas adjuntas como requisitos previos. A continuación, puede usar el AWS CLI para especificar el bucket, el tema y el rol. AWS Config Siga este procedimiento para configurar sus requisitos previos para AWS Config.

Temas

- Paso 1: crear un bucket de Amazon S3
- Paso 2: crear un tema de Amazon SNS
- Paso 3: crear un rol de IAM

Paso 1: crear un bucket de Amazon S3

Si ya tiene un bucket de Amazon S3 en su cuenta y desea utilizarlo, omita este paso y vaya a Paso 2: crear un tema de Amazon SNS.

Uso de la consola de S3

Creación de un bucket

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Elija Crear bucket.
3. En Nombre del bucket, escriba un nombre compatible con DNS para el bucket.

   El nombre del bucket debe:

   - Ser único en todo Amazon S3.
   - Tener entre 3 y 63 caracteres.
   - No contiene caracteres en mayúsculas.
   - Comenzar por una letra minúscula o un número.

   Una vez que haya creado el bucket, no podrá modificar su nombre. Asegúrese de que el nombre del bucket que elija sea único entre todos los nombres de buckets de Amazon S3. Para obtener más información acerca de las convenciones de nomenclatura de buckets de Amazon S3, consulte Restricciones y limitaciones de los buckets en la Guía del usuario de Amazon Simple Storage Service.

   > **Important**
   >
   > No incluya información confidencial en el nombre del bucket. El nombre del depósito está visible URLs cuando apunta a los objetos del depósito.

4. En Región, elige la AWS región en la que quieres que resida el depósito.

   Puede seleccionar una región cercana para minimizar la latencia y los costos, así como para satisfacer los requisitos reglamentarios. Los objetos almacenados en una región nunca abandonarán esa región salvo que usted los transfiera de forma específica a otra. Para obtener una lista de AWS las regiones de Amazon S3, consulte los puntos AWS de enlace del Referencia general de Amazon Web Servicesservicio en.

5. En Configuración del bucket para Block Public Access, elija la configuración de Block Public Access que desee aplicar al bucket.

   Le recomendamos que deje todas las configuraciones habilitadas a menos que sepa que necesita desactivar una o varias de ellas para su caso de uso, como alojar un sitio web público. La configuración de acceso público de bloqueo que habilite para el bucket también se habilitará para todos los puntos de acceso que cree en el bucket. Para obtener más información acerca del bloqueo de acceso público, consulte Usar el bloqueo de acceso público de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

6. (Opcional) Si desea habilitar Bloqueo de objetos en S3, realice las siguientes acciones:

   a. Elija Configuración avanzada y lea el mensaje que aparece.

   > **Important**
   >
   > Solo se puede habilitar Bloqueo de objetos en S3 para un bucket cuando se crea. Si habilita Bloqueo de objetos para el bucket, no podrá deshabilitarlo más adelante. Al habilitar Bloqueo de objetos, también se habilita el control de versiones para el bucket. Después de habilitar Bloqueo de objetos para el bucket, debe configurar los valores de Bloqueo de objetos antes de proteger los objetos del bucket. Para obtener más información acerca de cómo configurar la protección para objetos, consulte Configuring S3 Object Lock using the Amazon S3 console.

   b. Si desea habilitar el bloqueo de objetos, escriba enable (habilitar) en el cuadro de texto y elija Confirm (Confirmar).

   Para obtener más información acerca de la función Bloqueo de objetos en S3, consulte Usar Bloqueo de objetos de S3 en la Guía del usuario de Amazon Simple Storage Service.

7. Elija Crear bucket.

Usando el AWS SDKs

Al utilizar el AWS SDKs para crear un depósito, debe crear un cliente y, a continuación, utilizar el cliente para enviar una solicitud de creación de un depósito. Como práctica recomendada, debe crear el cliente y el bucket en la misma Región de AWS. Si no especifica una región al crear un cliente o un bucket, Amazon S3 utiliza la región predeterminada, EE. UU. Este (Norte de Virginia).

Para crear un cliente que pueda acceder a un punto final de doble pila, debe especificar un Región de AWS. Para obtener más información, consulte Puntos de enlace de doble pila en Amazon S3. Para obtener una lista de los disponibles Regiones de AWS, consulte Regiones y puntos finales en el. Referencia general de AWS

Al crear un cliente, la región se asigna al punto de conexión específico de la región. El cliente utiliza este punto de conexión para comunicarse con Amazon S3: `s3.<region>.amazonaws.com`. Si su región se lanzó después del 20 de marzo de 2019, su cliente y el bucket deben estar en la misma región. Sin embargo, puede utilizar un cliente en la región EE. UU. Este (Norte de Virginia) para crear un bucket en cualquier región que se haya lanzado antes del 20 de marzo de 2019. Para obtener más información, consulte Puntos de conexión heredados.

Estos ejemplos de código del AWS SDK realizan las siguientes tareas:

- Crear un cliente mediante la especificación explícita de una Región de AWS: en el ejemplo, el cliente utiliza el punto de conexión `s3.us-west-2.amazonaws.com` para comunicarse con Amazon S3. Puede especificar cualquier Región de AWS. Para obtener una lista Regiones de AWS, consulte Regiones y puntos finales en la Referencia AWS general.
- Enviar una solicitud de creación de bucket al especificar solo un nombre de bucket: el cliente envía una solicitud a Amazon S3 para crear el bucket en la región donde usted creó un cliente.
- Recuperar la información acerca de la ubicación del bucket: Amazon S3 almacena información de la ubicación del bucket en el subrecurso location asociado con el bucket.

Los siguientes ejemplos de código muestran cómo utilizar `CreateBucket`.

.NET

SDK para .NET (v4)

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
/// <summary>
/// Shows how to create a new Amazon S3 bucket.
```

```
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <returns>A boolean value representing the success or failure of
    /// the bucket creation process.</returns>
    public async Task<bool> CreateBucketAsync(string bucketName)
    {
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
            };

            var response = await _amazonS3.PutBucketAsync(request);
            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- Para obtener más información sobre la API, consulta CreateBucketla Referencia AWS SDK para .NET de la API.

SDK para .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree un nuevo bucket con el bloqueo de objetos habilitado.

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
```

```
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- Para obtener más información sobre la API, consulta CreateBucketla Referencia AWS SDK para .NET de la API.

Bash

AWS CLI con el script Bash

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
##############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
```

```
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi

  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""
```

```
  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- Para obtener más información sobre la API, consulta CreateBucketla Referencia de AWS CLI comandos.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
bool AwsDoc::S3::createBucket(const Aws::String &bucketName,
                              const Aws::S3::S3ClientConfiguration &clientConfig)
 {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    if (clientConfig.region != "us-east-1") {
```

```
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: createBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    } else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Para obtener más información sobre la API, consulta CreateBucketla Referencia AWS SDK para C++ de la API.

CLI

AWS CLI

Ejemplo 1: Creación de un bucket

En los siguientes ejemplos de `create-bucket` se crea un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1
```

Salida:

```
{
```

```
    "Location": "/amzn-s3-demo-bucket"
}
```

Para obtener más información, consulte Crear un bucket en la Guía del usuario de Amazon S3.

Ejemplo 2: Creación de un bucket con propietario obligatorio

En el siguiente ejemplo de `create-bucket` se crea un bucket denominado `amzn-s3-demo-bucket` que utiliza la configuración Aplicada al propietario del bucket de S3 Object Ownership.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

Salida:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

Para obtener más información, consulte Control de la propiedad de objetos y desactivación ACLs en la Guía del usuario de Amazon S3.

Ejemplo 3: creación de un bucket fuera de la región us-east-1

En el siguiente ejemplo `create-bucket`, se crea un bucket denominado `amzn-s3-demo-bucket` en la región `eu-west-1`. Las regiones situadas fuera de `us-east-1` requieren que se especifique el `LocationConstraint` correspondiente para poder crear el bucket en la región deseada.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

Salida:

```
{
```

```
    "Location": "http://amzn-s3-demo-bucket.s3.amazonaws.com/"
}
```

Para obtener más información, consulte Crear un bucket en la Guía del usuario de Amazon S3.

- Para obtener más información sobre la API, consulte CreateBucketla Referencia de AWS CLI comandos.

Go

SDK para Go V2

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree un bucket con la configuración predeterminada.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
```

```
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(ctx context.Context, name string, region
 string) error {
 _, err := basics.S3Client.CreateBucket(ctx, &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", name)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", name)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(name)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", name)
  }
 }
 return err
}
```

Cree un bucket con el bloqueo de objetos y espere a que aparezca.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// S3Actions wraps S3 service actions.
type S3Actions struct {
 S3Client  *s3.Client
 S3Manager *manager.Uploader
}



// CreateBucketWithLock creates a new S3 bucket with optional object locking
 enabled
// and waits for the bucket to exist before returning.
func (actor S3Actions) CreateBucketWithLock(ctx context.Context, bucket string,
 region string, enableObjectLock bool) (string, error) {
 input := &s3.CreateBucketInput{
  Bucket: aws.String(bucket),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 }

 if enableObjectLock {
  input.ObjectLockEnabledForBucket = aws.Bool(true)
 }

 _, err := actor.S3Client.CreateBucket(ctx, input)
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
```

```
    log.Printf("You already own bucket %s.\n", bucket)
    err = owned
   } else if errors.As(err, &exists) {
    log.Printf("Bucket %s already exists.\n", bucket)
    err = exists
   }
  } else {
   err = s3.NewBucketExistsWaiter(actor.S3Client).Wait(
    ctx, &s3.HeadBucketInput{Bucket: aws.String(bucket)}, time.Minute)
   if err != nil {
    log.Printf("Failed attempt to wait for bucket %s to exist.\n", bucket)
   }
  }

  return bucket, err
 }
```

- Para obtener más información sobre la API, consulta CreateBucketla Referencia AWS SDK para Go de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Crear un bucket.

```
    /**
     * Creates an S3 bucket asynchronously.
     *
     * @param bucketName the name of the S3 bucket to create
     * @return a {@link CompletableFuture} that completes when the bucket is
 created and ready
     * @throws RuntimeException if there is a failure while creating the bucket
```

```
     */
    public CompletableFuture<Void> createBucketAsync(String bucketName) {
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .build();

        CompletableFuture<CreateBucketResponse> response =
getAsyncClient().createBucket(bucketRequest);
        return response.thenCompose(resp -> {
            S3AsyncWaiter s3Waiter = getAsyncClient().waiter();
            HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
                .bucket(bucketName)
                .build();

            CompletableFuture<WaiterResponse<HeadBucketResponse>>
waiterResponseFuture =
                s3Waiter.waitUntilBucketExists(bucketRequestWait);
            return waiterResponseFuture.thenAccept(waiterResponse -> {
                waiterResponse.matched().response().ifPresent(headBucketResponse
-> {
                    logger.info(bucketName + " is ready");
                });
            });
        }).whenComplete((resp, ex) -> {
            if (ex != null) {
                throw new RuntimeException("Failed to create bucket", ex);
            }
        });
    }
```

Cree un nuevo bucket con el bloqueo de objetos habilitado.

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();

        getClient().createBucket(bucketRequest);
```

```
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- Para obtener más información sobre la API, consulta CreateBucketla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Crear el bucket.

```
import {
  BucketAlreadyExists,
  BucketAlreadyOwnedByYou,
  CreateBucketCommand,
  S3Client,
  waitUntilBucketExists,
} from "@aws-sdk/client-s3";

/**
 * Create an Amazon S3 bucket.
 * @param {{ bucketName: string }} config
 */
export const main = async ({ bucketName }) => {
  const client = new S3Client({});

  try {
```

```
    const { Location } = await client.send(
      new CreateBucketCommand({
        // The name of the bucket. Bucket names are unique and have several other
 constraints.
        // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
        Bucket: bucketName,
      }),
    );
    await waitUntilBucketExists({ client }, { Bucket: bucketName });
    console.log(`Bucket created with location ${Location}`);
  } catch (caught) {
    if (caught instanceof BucketAlreadyExists) {
      console.error(
        `The bucket "${bucketName}" already exists in another AWS account. Bucket
 names must be globally unique.`,
      );
    }
    // WARNING: If you try to create a bucket in the North Virginia region,
    // and you already own a bucket in that region with the same name, this
    // error will not be thrown. Instead, the call will return successfully
    // and the ACL on that bucket will be reset.
    else if (caught instanceof BucketAlreadyOwnedByYou) {
      console.error(
        `The bucket "${bucketName}" already exists in this AWS account.`,
      );
    } else {
      throw caught;
    }
  }
};
```

- Para obtener más información, consulte la Guía para desarrolladores de AWS SDK para JavaScript.
- Para obtener más información sobre la API, consulta CreateBucketla Referencia AWS SDK para JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client.fromEnvironment { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- Para obtener más información sobre la API, consulta CreateBucketla referencia sobre el AWS SDK para la API de Kotlin.

PHP

SDK para PHP

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Crear un bucket.

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);
```

```
        try {
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
 $exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- Para obtener más información sobre la API, consulta CreateBucketla Referencia AWS SDK para PHP de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree un bucket con la configuración predeterminada.

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
```

```
        """
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

Cree un bucket con control de versiones con una configuración de ciclo de vida.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.
```

```
    Usage is shown in the usage_demo_single_object function at the end of this
module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
```

```
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- Para obtener más información sobre la API, consulta CreateBucketla AWS Referencia de API de SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket
```

```
  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end
```

```
run_demo if $PROGRAM_NAME == __FILE__
```

- Para obtener más información sobre la API, consulta CreateBucketla Referencia AWS SDK para Ruby de la API.

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
pub async fn create_bucket(
    client: &aws_sdk_s3::Client,
    bucket_name: &str,
    region: &aws_config::Region,
) -> Result<Option<aws_sdk_s3::operation::create_bucket::CreateBucketOutput>,
 S3ExampleError> {
    let constraint =
 aws_sdk_s3::types::BucketLocationConstraint::from(region.to_string().as_str());
    let cfg = aws_sdk_s3::types::CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    let create = client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await;

    // BucketAlreadyExists and BucketAlreadyOwnedByYou are not problems for this
 task.
    create.map(Some).or_else(|err| {
        if err
            .as_service_error()
```

```
            .map(|se| se.is_bucket_already_exists() ||
 se.is_bucket_already_owned_by_you())
            == Some(true)
        {
            Ok(None)
        } else {
            Err(S3ExampleError::from(err))
        }
    })
}
```

- Para obtener más información sobre la API, consulta CreateBucketla referencia sobre la API de AWS SDK para Rust.

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    TRY.
        " determine our region from our session
        DATA(lv_region) = CONV /aws1/s3_bucketlocationcnstrnt( lo_session-
>get_region( ) ).
        DATA lo_constraint TYPE REF TO /aws1/cl_s3_createbucketconf.
        " When in the us-east-1 region, you must not specify a constraint
        " In all other regions, specify the region as the constraint
        IF lv_region = 'us-east-1'.
          CLEAR lo_constraint.
        ELSE.
          lo_constraint = NEW /aws1/cl_s3_createbucketconf( lv_region ).
        ENDIF.

        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
            io_createbucketconfiguration  = lo_constraint ).
```

```
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- Para obtener más información sobre la API, consulte CreateBucketla referencia sobre la API ABAP del AWS SDK para SAP.

Swift

SDK para Swift

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import AWSS3

    public func createBucket(name: String) async throws {
        var input = CreateBucketInput(
            bucket: name
        )

        // For regions other than "us-east-1", you must set the
 locationConstraint in the createBucketConfiguration.
        // For more information, see LocationConstraint in the S3 API guide.
        // https://docs.aws.amazon.com/AmazonS3/latest/API/
API_CreateBucket.html#API_CreateBucket_RequestBody
        if let region = configuration.region {
            if region != "us-east-1" {
                input.createBucketConfiguration =
 S3ClientTypes.CreateBucketConfiguration(locationConstraint:
 S3ClientTypes.BucketLocationConstraint(rawValue: region))
            }
        }
```

```
        do {
            _ = try await client.createBucket(input: input)
        }
        catch let error as BucketAlreadyOwnedByYou {
            print("The bucket '\(name)' already exists and is owned by you. You
may wish to ignore this exception.")
            throw error
        }
        catch {
            print("ERROR: ", dump(error, name: "Creating a bucket"))
            throw error
        }
    }
```

- Para obtener más información sobre la API, consulta CreateBucketla referencia sobre la API de AWS SDK for Swift.

> **Note**
>
> También puede utilizar un bucket de Amazon S3 desde una cuenta diferente, pero es posible que deba crear una política para el bucket que otorgue permisos de acceso a AWS Config. Para obtener más información sobre la concesión de permisos a un bucket de Amazon S3, consulte Permisos del bucket de Amazon S3 para el canal AWS Config de entrega y, a continuación, vaya a Paso 2: crear un tema de Amazon SNS.

Paso 2: crear un tema de Amazon SNS

Si ya tiene un tema de Amazon SNS en su cuenta y desea utilizarlo, omita este paso y vaya a Paso 3: crear un rol de IAM.

Uso de la consola de SNS

Para crear un tema de Amazon SNS

1. Abra la consola Amazon SNS en https://console.aws.amazon.com/sns/ la versión 3/home.
2. Realice una de las siguientes acciones:

- Si nunca se ha creado ningún tema bajo tu Cuenta de AWS dirección, lee la descripción de Amazon SNS en la página de inicio.

- Si los temas se han creado Cuenta de AWS anteriormente bajo su dirección, en el panel de navegación, elija Temas.

3. En la página Temas, elija Crear tema.
4. En la página Crear tema, en la sección Detalles, haga lo siguiente:
   a. Para Tipo, elija un tipo de tema (estándar o FIFO).
   b. Ingrese un nombre para el nuevo tema. En el caso de un tema FIFO, agregue .fifo al final del nombre.
   c. (Opcional) Ingrese un nombre para mostrar para el tema.
   d. (Opcional) En el caso de un tema FIFO, puede elegir Desduplicación de mensajes basada en el contenido para habilitar la desduplicación de mensajes predeterminada. Para obtener más información, consulte Desduplicación de mensajes para temas FIFO.
5. (Opcional) Expanda la sección Encryption (Cifrado) y haga lo siguiente. Para obtener más información, consulte Cifrado en reposo.
   a. Elija Habilitar el cifrado.
   b. Especifique la clave maestra del cliente (CMK). Para obtener más información, consulte Términos clave.

      Se muestran los valores de Description (Descripción), Account (Cuenta) y CMK ARN (ARN de CMK) de cada CMK.

      > **Important**
      >
      > Si no es el propietario de la CMK o si ha iniciado sesión con una cuenta que no tiene los permisos `kms:ListAliases` y `kms:DescribeKey`, no podrá ver la información sobre la CMK en la consola de Amazon SNS.
      > Pida al propietario de la CMK que le conceda estos permisos. Para obtener más información, consulte Permisos API de AWS KMS : referencia de recursos y acciones en la Guía para desarrolladores de AWS Key Management Service .

- La CMK AWS gestionada para Amazon SNS (predeterminadaalias/aws/sns) está seleccionada de forma predeterminada.

> **Note**
>
> Tenga en cuenta lo siguiente:
>
> - La primera vez que utilice Consola de administración de AWS para especificar la CMK AWS gestionada para Amazon SNS para un tema AWS KMS , crea AWS la CMK gestionada para Amazon SNS.
> - Como alternativa, la primera vez que utilice la `Publish` acción en un tema con SSE habilitado, se AWS KMS creará la CMK AWS gestionada para Amazon SNS.

- Para usar una CMK personalizada suya Cuenta de AWS, elija el campo Clave maestra del cliente (CMK) y, a continuación, elija la CMK personalizada de la lista.

> **Note**
>
> Para obtener instrucciones sobre cómo crear claves personalizadas CMKs, consulte Creación de claves en la Guía para desarrolladores AWS Key Management Service

- Para usar un ARN CMK personalizado de Cuenta de AWS su cuenta o de AWS otra, introdúzcalo en el campo Clave maestra del cliente (CMK).

6. (Opcional) De forma predeterminada, solo el propietario del tema puede publicar en el tema o suscribirse a este. Para configurar permisos de acceso adicionales, expanda la sección Access policy (Política de acceso). Para obtener más información, consulte ¿Qué es Amazon SNS? y Ejemplos de casos de control de acceso con Amazon SNS.

> **Note**
>
> Cuando se crea un tema a través de la consola, la política predeterminada utiliza la clave de condición `aws:SourceOwner`. Esta clave es similar a `aws:SourceAccount`.

7. (Opcional) Para configurar la forma en que Amazon SNS reintenta los intentos de entrega de mensajes con error, expanda la sección Política de reintentos de entrega (HTTP/S). Para obtener más información, consulte Reintento de entrega de mensajes de Amazon SNS.
8. (Opcional) Para configurar la forma en que Amazon SNS registra la entrega de mensajes CloudWatch, amplíe la sección Registro del estado de entrega. Para obtener más información, consulte Estado de entrega de mensajes de Amazon SNS.
9. (Opcional) Para añadir etiquetas de metadatos al tema, expanda la sección Tags (Etiquetas), escriba un valor en Key (Clave) y en Value (Valor) (opcional) y elija Add tag (Añadir etiqueta). Para obtener más información, consulte Etiquetado de temas de Amazon SNS.
10. Seleccione Crear tema.

    Se crea el tema y se muestra la ***MyTopic***página.

    En la sección Detalles se muestran el Name del tema, ARN, (opcional) Nombre para mostrar e ID de cuenta de AWS del Propietario del tema.
11. Copie el ARN del tema en el portapapeles, por ejemplo:

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

Para suscribir una dirección de correo electrónico al tema de Amazon SNS

1. Abra la consola Amazon SNS en https://console.aws.amazon.com/sns/ la versión 3/home.
2. En el panel de navegación izquierdo, elija Suscripciones.
3. En la página Subscriptions (Suscripciones), elija Create subscription (Crear suscripción).
4. En la página Crear suscripción, en la sección Detalles, haga lo siguiente:
   a. En ARN de tema, elija el nombre de recurso de Amazon (ARN) de un tema.
   b. En Protocolo, elija un tipo de punto de enlace. Los tipos de puntos de enlace disponibles son:
      - HTTP/HTTPS
      - Correo electrónico/Correo electrónico JSON
      - Amazon Data Firehose
      - Amazon SQS

> **Note**
>
> Para suscribirse a un tema de SNS FIFO, elija esta opción.

- AWS Lambda
- Punto de conexión de aplicación de plataforma
- SMS

c. En Punto de enlace, ingrese el valor del punto de enlace, como una dirección de correo electrónico o el ARN de una cola de Amazon SQS.

d. Solo para los puntos de conexión de Firehose: en ARN del rol de suscripción, especifique el ARN del rol de IAM que creó para escribir en flujos de entrega de Firehose. Para obtener más información, consulte Prerequisites for subscribing Firehose delivery streams to Amazon SNS topics.

e. (Opcional) Para los puntos de conexión Firehose, Amazon SQS y otros terminales HTTP/S , también puede habilitar la entrega de mensajes sin procesar. Para obtener más información, consulte Entrega de mensajes sin procesar de Amazon SNS.

f. (Opcional) Para configurar una política de filtro, expanda la sección Política de filtro de suscripción. Para obtener más información, consulte Políticas de filtro de suscripciones de Amazon SNS.

g. (Opcional) Para configurar una cola de mensajes fallidos en la suscripción, expanda la sección Política de reconducción (cola de mensajes fallidos). Para obtener más información, consulte las colas de cartas muertas de Amazon SNS (). DLQs

h. Seleccione Crear subscripción.

   En la consola se crea la suscripción y se abre la página Detalles de la suscripción.

Usando el AWS SDKs

Para usar un AWS SDK, debe configurarlo con sus credenciales. Para obtener más información, consulte Los archivos de configuración y credenciales compartidos en la Guía de referencia de herramientas AWS SDKs y herramientas.

Los siguientes ejemplos de código muestran cómo utilizar `CreateTopic`.

.NET

SDK para .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree un tema con un nombre específico.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.SimpleNotificationService;
    using Amazon.SimpleNotificationService.Model;

    /// <summary>
    /// This example shows how to use Amazon Simple Notification Service
    /// (Amazon SNS) to add a new Amazon SNS topic.
    /// </summary>
    public class CreateSNSTopic
    {
        public static async Task Main()
        {
            string topicName = "ExampleSNSTopic";

            IAmazonSimpleNotificationService client = new
 AmazonSimpleNotificationServiceClient();

            var topicArn = await CreateSNSTopicAsync(client, topicName);
            Console.WriteLine($"New topic ARN: {topicArn}");
        }

        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
```

```
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

Cree un tema nuevo con un nombre y atributos específicos de FIFO y desduplicación.

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
        };

        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }
```

```
            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
 "true");
            }
        }

        var createResponse = await
 _amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- Para obtener más información sobre la API, consulta CreateTopicla Referencia AWS SDK para .NET de la API.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
/*!
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
```

```
                                const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }

    return outcome.IsSuccess();
}
```

- Para obtener más información sobre la API, consulta CreateTopicla Referencia AWS SDK para C++ de la API.

CLI

AWS CLI

Creación de un tema de SNS

En el siguiente ejemplo de `create-topic` se crea un tema de SNS denominado `my-topic`.

```
aws sns create-topic \
    --name my-topic
```

Salida:

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

Para obtener más información, consulte Uso de la interfaz de línea de AWS comandos con Amazon SQS y Amazon SNS en la Guía del usuario de AWS la interfaz de línea de comandos.

- Para obtener más información sobre la API, consulte la Referencia CreateTopicde AWS CLI comandos.

Go

SDK para Go V2

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/sns"
 "github.com/aws/aws-sdk-go-v2/service/sns/types"
)

// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}
```

```
// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(ctx context.Context, topicName string,
 isFifoTopic bool, contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(ctx, &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- Para obtener más información sobre la API, consulta CreateTopicla Referencia AWS SDK para Go de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }
```

```
        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- Para obtener más información sobre la API, consulta CreateTopicla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurarlo y ejecutarlo en el Repositorio de ejemplos de código de AWS.

Cree el cliente en un módulo separado y expórtelo.

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

Importe el SDK y los módulos cliente, y llame a la API.

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- Para obtener información, consulte la Guía para desarrolladores de AWS SDK para JavaScript.
- Para obtener más información sobre la API, consulta CreateTopicla Referencia AWS SDK para JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient.fromEnvironment { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
}
```

- Para obtener más información sobre la API, consulta CreateTopicla referencia sobre el AWS SDK para la API de Kotlin.

PHP

SDK para PHP

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
```

```
use Aws\Sns\SnsClient;


/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- Para obtener más información, consulte la Guía para desarrolladores de AWS SDK para PHP.
- Para obtener más información sobre la API, consulta CreateTopicla Referencia AWS SDK para PHP de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource


    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

```
class SnsWrapper:
    """Wrapper class for managing Amazon SNS operations."""

    def __init__(self, sns_client: Any) -> None:
```

```
        """
        Initialize the SnsWrapper.

        :param sns_client: A Boto3 Amazon SNS client.
        """
        self.sns_client = sns_client

    @classmethod
    def from_client(cls) -> 'SnsWrapper':
        """
        Create an SnsWrapper instance using a default boto3 client.

        :return: An instance of this class.
        """
        sns_client = boto3.client('sns')
        return cls(sns_client)


    def create_topic(
        self,
        topic_name: str,
        is_fifo: bool = False,
        content_based_deduplication: bool = False
    ) -> str:
        """
        Create an SNS topic.

        :param topic_name: The name of the topic to create.
        :param is_fifo: Whether to create a FIFO topic.
        :param content_based_deduplication: Whether to use content-based
deduplication for FIFO topics.
        :return: The ARN of the created topic.
        :raises ClientError: If the topic creation fails.
        """
        try:
            # Add .fifo suffix for FIFO topics
            if is_fifo and not topic_name.endswith('.fifo'):
                topic_name += '.fifo'

            attributes = {}
            if is_fifo:
                attributes['FifoTopic'] = 'true'
                if content_based_deduplication:
                    attributes['ContentBasedDeduplication'] = 'true'
```

```
            response = self.sns_client.create_topic(
                Name=topic_name,
                Attributes=attributes
            )

            topic_arn = response['TopicArn']
            logger.info(f"Created topic: {topic_name} with ARN: {topic_arn}")
            return topic_arn

        except ClientError as e:
            error_code = e.response.get('Error', {}).get('Code', 'Unknown')
            logger.error(f"Error creating topic {topic_name}: {error_code} -
 {e}")
            raise
```

- Para obtener más información sobre la API, consulta CreateTopicla AWS Referencia de API de SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end
```

```
  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = 'YourTopicName' # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
  unless sns_topic_creator.create_topic(topic_name)
    puts 'The topic was not created. Stopping program.'
    exit 1
  end
end
```

- Para obtener más información, consulte la Guía para desarrolladores de AWS SDK para Ruby.
- Para obtener más información sobre la API, consulta CreateTopicla Referencia AWS SDK para Ruby de la API.

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- Para obtener más información sobre la API, consulta CreateTopicla referencia sobre la API de AWS SDK para Rust.

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    TRY.
        oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
 is returned for testing purposes. "
        MESSAGE 'SNS topic created' TYPE 'I'.
      CATCH /aws1/cx_snstopiclimitexcdex.
```

```
        MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
    ENDTRY.
```

- Para obtener más información sobre la API, consulte CreateTopicla referencia sobre la API ABAP del AWS SDK para SAP.

Swift

SDK para Swift

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import AWSSNS

        let config = try await SNSClient.SNSClientConfiguration(region: region)
        let snsClient = SNSClient(config: config)

        let output = try await snsClient.createTopic(
            input: CreateTopicInput(name: name)
        )

        guard let arn = output.topicArn else {
            print("No topic ARN returned by Amazon SNS.")
            return
        }
```

- Para obtener más información sobre la API, consulta CreateTopicla referencia sobre la API de AWS SDK for Swift.

> **Note**
>
> También puede utilizar un tema de Amazon SNS de otra cuenta, pero es posible que tenga que crear una política para el tema que conceda permisos de acceso a AWS Config. Para

obtener información sobre la concesión de permisos a un tema de Amazon SNS, consulte Permisos para el tema de Amazon SNS y, a continuación, vaya a Paso 3: crear un rol de IAM.

Paso 3: crear un rol de IAM

> **Important**
>
> (Recomendado) Usa el rol vinculado al AWS Config servicio
> Se recomienda utilizar el rol vinculado al AWS Config servicio:.
> `AWSServiceRoleForConfig` Los roles vinculados al servicio están predefinidos e incluyen todos los permisos necesarios para llamar a otros AWS Config . Servicios de AWS El rol AWS Config vinculado al servicio es obligatorio para los grabadores de configuración vinculados al servicio.
> Para obtener más información, consulte Uso de roles vinculados a servicios para AWS Config.

Uso de la consola de IAM

Puede usar la consola de IAM para crear un rol de IAM que conceda AWS Config permisos para acceder a su bucket de Amazon S3, acceder a su tema de Amazon SNS y obtener detalles de configuración de los recursos compatibles. AWS Al utilizar la consola para crear un rol de IAM, AWS Config asocia automáticamente los permisos necesarios al rol en su nombre.

> **Note**
>
> Si ha utilizado un AWS servicio que utiliza AWS Config (como AWS Security Hub o AWS Control Tower) y ya se ha creado un AWS Config rol, debe asegurarse de que el rol de IAM que utilice al configurar AWS Config mantenga los mismos privilegios mínimos que el AWS Config rol ya creado para que el otro AWS servicio siga ejecutándose según lo previsto.
> Por ejemplo, si AWS Control Tower tiene una función de IAM que AWS Config permite leer los objetos de Amazon S3, debe garantizar que se concedan los mismos permisos en la función de IAM que utilizó al configurar. AWS Config De lo contrario, podría interferir con las operaciones AWS de Control Tower.

Para obtener más información sobre las funciones de IAM AWS Config, consulte AWS Identity and Access Management.

Para crear un rol para un servicio AWS

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, elija Crear rol.
3. En Select trusted entity (Seleccionar entidad de confianza), elija AWS service (Servicio de).
4. Elige el caso de uso que desees para AWS Config: Config - Customizable, Config - Organizations, Config o Config - Conformance Packs. A continuación, elija Siguiente.
5. En la página Asignar nombre, revisar y crear, revise los datos de su rol y elija Crear rol.

Usando el AWS SDKs

Para usar un AWS SDK, debe configurarlo con sus credenciales. Para obtener más información, consulte Los archivos de configuración y credenciales compartidos en la Guía de referencia de herramientas AWS SDKs y herramientas.

Los siguientes ejemplos de código muestran cómo utilizar `CreateRole`.

.NET

SDK para .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
/// <summary>
/// Create a new IAM role.
/// </summary>
/// <param name="roleName">The name of the IAM role.</param>
/// <param name="rolePolicyDocument">The name of the IAM policy document
```

```
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
 rolePolicyDocument)
    {
        var request = new CreateRoleRequest
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- Para obtener más información sobre la API, consulta CreateRolela Referencia AWS SDK para .NET de la API.

Bash

AWS CLI con el script Bash

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
```

```
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_json -- The assume role policy document."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_document="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1
```

```
  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_document" ]]; then
    errecho "ERROR: You must provide a policy document with the -p parameter."
    usage
    return 1
  fi

  response=$(aws iam create-role \
    --role-name "$role_name" \
    --assume-role-policy-document "$policy_document" \
    --output text \
    --query Role.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener más información sobre la API, consulta CreateRolela Referencia de AWS CLI comandos.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;

    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Para obtener más información sobre la API, consulta CreateRolela Referencia AWS SDK para C++ de la API.

CLI

AWS CLI

Ejemplo 1: cómo crear un rol de IAM

El siguiente comando `create-role` crean un rol denominado `Test-Role` y le asocia una política de confianza.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

Salida:

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

La política de confianza se define como un documento JSON en el archivo Test-Role-Trust-Policy.json. (El nombre y la extensión del archivo no son significativos). La política de confianza debe especificar una entidad principal.

Utilice el comando `put-role-policy` para asociar una política de permisos a un rol.

Para más información, consulte Creación de roles de IAM en la Guía del usuario de IAM de AWS .

Ejemplo 2: cómo crear un rol de IAM con una duración máxima de sesión especificada

El siguiente comando `create-role` crea un rol denominado `Test-Role` y establece una duración máxima de sesión de 7200 segundos (2 horas).

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
```

```
    --max-session-duration 7200
```

Salida:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Para obtener más información, consulte Modificación de la duración máxima de sesión (AWS API) de un rol en la Guía del usuario de AWS IAM.

Ejemplo 3: cómo crear un rol de IAM con etiquetas

El siguiente comando crea un rol de IAM `Test-Role` con etiquetas. En este ejemplo, se utiliza el indicador de parámetro `--tags` con las siguientes etiquetas con formato JSON: `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`. Alternativamente, el indicador `--tags` se puede usar con etiquetas en formato abreviado: `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
```

```
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Salida:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

Para obtener más información, consulte Etiquetado de roles de IAM en la Guía del usuario de AWS IAM.

- Para obtener más información sobre la API, consulte CreateRolela Referencia de AWS CLI comandos.

Go

SDK para Go V2

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/iam"
 "github.com/aws/aws-sdk-go-v2/service/iam/types"
)

// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(ctx context.Context, roleName string,
 trustedUserArn string) (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version: "2012-10-17",
  Statement: []PolicyStatement{{
```

```
    Effect:    "Allow",
    Principal: map[string]string{"AWS": trustedUserArn},
    Action:    []string{"sts:AssumeRole"},
   }},
  }
  policyBytes, err := json.Marshal(trustPolicy)
  if err != nil {
   log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
  trustedUserArn, err)
   return nil, err
  }
  result, err := wrapper.IamClient.CreateRole(ctx, &iam.CreateRoleInput{
   AssumeRolePolicyDocument: aws.String(string(policyBytes)),
   RoleName:                 aws.String(roleName),
  })
  if err != nil {
   log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
  } else {
   role = result.Role
  }
  return role, err
 }
```

- Para obtener más información sobre la API, consulta CreateRolela Referencia AWS SDK para Go de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
```

```
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
                    rolename - The name of the role to create.\s
                    fileLocation - The location of the JSON document that
 represents the trust policy.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
        IamClient iam = IamClient.builder()
                .region(region)
                .build();
```

```
        String result = createIAMRole(iam, rolename, fileLocation);
        System.out.println("Successfully created user: " + result);
        iam.close();
    }

    public static String createIAMRole(IamClient iam, String rolename, String
 fileLocation) throws Exception {
        try {
            JSONObject jsonObject = (JSONObject)
 readJsonSimpleDemo(fileLocation);
            CreateRoleRequest request = CreateRoleRequest.builder()
                    .roleName(rolename)
                    .assumeRolePolicyDocument(jsonObject.toJSONString())
                    .description("Created using the AWS SDK for Java")
                    .build();

            CreateRoleResponse response = iam.createRole(request);
            System.out.println("The ARN of the role is " +
 response.role().arn());

        } catch (IamException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }

    public static Object readJsonSimpleDemo(String filename) throws Exception {
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- Para obtener más información sobre la API, consulta CreateRolela Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Creación del rol.

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
      ],
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- Para obtener más información sobre la API, consulta CreateRolela Referencia AWS SDK para JavaScript de la API.

PHP

SDK para PHP

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
```

```
            ]);
        });
        return $result['Role'];
    }
```

- Para obtener más información sobre la API, consulta CreateRolela Referencia AWS SDK para PHP de la API.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: en este ejemplo se crea un nuevo rol con el nombre **MyNewRole** y se le adjunta la política que se encuentra en el archivo **NewRoleTrustPolicy.json**. Tenga en cuenta que debe usar el parámetro de conmutación **-Raw** para procesar correctamente el archivo de políticas JSON. El documento de política que se muestra en el resultado tiene codificación de URL. En este ejemplo, se decodifica con el método **UrlDecode** de .NET.

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

Salida:

```
Arn                       : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                           %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                           %20%5D%0D%0A%7D
CreateDate                : 4/15/2015 11:04:23 AM
```

```
Path                      : /
RoleId                    : V5PAJI2KPN4EAEXAMPLE1
RoleName                  : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Para obtener más información sobre la API, consulte CreateRole Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: en este ejemplo se crea un nuevo rol con el nombre **`MyNewRole`** y se le adjunta la política que se encuentra en el archivo **`NewRoleTrustPolicy.json`**. Tenga en cuenta que debe usar el parámetro de conmutación **`-Raw`** para procesar correctamente el archivo de políticas JSON. El documento de política que se muestra en el resultado tiene codificación de URL. En este ejemplo, se decodifica con el método **`UrlDecode`** de .NET.

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

Salida:

```
Arn                       : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
```

```
                            %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                            %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                            %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                            %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                            %20%5D%0D%0A%7D
CreateDate                : 4/15/2015 11:04:23 AM
Path                      : /
RoleId                    : V5PAJI2KPN4EAEXAMPLE1
RoleName                  : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Para obtener más información sobre la API, consulte CreateRolela referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
        "Version":"2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- Para obtener más información sobre la API, consulta CreateRolela AWS Referencia de API de SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
 # Creates a role and attaches policies to it.
 #
 # @param role_name [String] The name of the role.
 # @param assume_role_policy_document [Hash] The trust relationship policy
document.
 # @param policy_arns [Array<String>] The ARNs of the policies to attach.
 # @return [String, nil] The ARN of the new role if successful, or nil if an
error occurred.
 def create_role(role_name, assume_role_policy_document, policy_arns)
   response = @iam_client.create_role(
     role_name: role_name,
     assume_role_policy_document: assume_role_policy_document.to_json
   )
   role_arn = response.role.arn

   policy_arns.each do |policy_arn|
     @iam_client.attach_role_policy(
       role_name: role_name,
       policy_arn: policy_arn
     )
   end

   role_arn
 rescue Aws::IAM::Errors::ServiceError => e
   @logger.error("Error creating role: #{e.message}")
   nil
 end
```

- Para obtener más información sobre la API, consulta CreateRolela Referencia AWS SDK para Ruby de la API.

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- Para obtener más información sobre la API, consulta CreateRolela referencia sobre la API de AWS SDK para Rust.

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    TRY.
        oo_result = lo_iam->createrole(
          iv_rolename = iv_role_name
          iv_assumerolepolicydocument = iv_assume_role_policy_document ).
        MESSAGE 'Role created successfully.' TYPE 'I'.
      CATCH /aws1/cx_iamentityalrdyexex.
        MESSAGE 'Role already exists.' TYPE 'E'.
      CATCH /aws1/cx_iammalformedplydocex.
        MESSAGE 'Assume role policy document is malformed.' TYPE 'E'.
      CATCH /aws1/cx_iamlimitexceededex.
        MESSAGE 'Role limit exceeded.' TYPE 'E'.
    ENDTRY.
```

- Para obtener más información sobre la API, consulte CreateRolela referencia sobre la API ABAP del AWS SDK para SAP.

Swift

SDK para Swift

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import AWSIAM
import AWSS3
```

```
    public func createRole(name: String, policyDocument: String) async throws ->
String {
        let input = CreateRoleInput(
            assumeRolePolicyDocument: policyDocument,
            roleName: name
        )
        do {
            let output = try await client.createRole(input: input)
            guard let role = output.role else {
                throw ServiceHandlerError.noSuchRole
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            print("ERROR: createRole:", dump(error))
            throw error
        }
    }
```

- Para obtener más información sobre la API, consulta CreateRolela referencia sobre la API de AWS SDK for Swift.

Inicio de AWS Config con un registrador de configuración administrado por el cliente utilizando la AWS CLI

Puede iniciar AWS Config creando un registrador de configuración administrado por el cliente. Para crear un registrador de configuración administrado por el cliente con la AWS CLI, utilice los siguientes comandos: `put-configuration-recorder`, `put-delivery-channel` y `start-configuration-recorder`.

- El comando `put-configuration-recorder` crea un registrador de configuración administrado por el cliente.
- El comando `put-delivery-channel` crea un objeto de canal de entrega en el que AWS Config entrega información de configuración a un bucket de S3 y un tema de SNS.

- El `start-configuration-recorder` inicia el registrador de configuración administrado por el cliente. El registrador de configuración administrado por el cliente comenzará a registrar los cambios de configuración de los tipos de recursos que especifique.

Temas

- Consideraciones
- Paso 1: ejecución de put-configuration-recorder
- Paso 2: ejecutar el comando put-delivery-channel
- Paso 3: ejecutar el comando start-configuration-recorder

Consideraciones

Se requieren un bucket de S3, un tema de SNS y una rol de IAM

Para crear un registrador de configuración administrado por el cliente, debe crear un bucket de Amazon S3, un tema de Amazon SNS y un rol de IAM con políticas asociadas como requisitos previos. Para configurar los requisitos previos para AWS Config, consulte Requisitos previos.

Un registrador de configuración administrado por el cliente por cuenta y región

Solo puede tener un registrador de configuración administrado por el cliente para cada Cuenta de AWS y cada Región de AWS.

Un canal de entrega por cuenta y región

Solo puede tener una región de canal de entrega para cada Cuenta de AWS y cada Región de AWS.

Políticas y resultados de cumplimiento

Las políticas de IAM y otras políticas administradas en AWS Organizations pueden afectar a los permisos de AWS Config para registrar cambios de configuración para los recursos. Además, las reglas evalúan directamente la configuración de un recurso y no tienen en cuenta estas políticas al ejecutar las evaluaciones. Asegúrese de que las políticas en vigor se ajusten a la forma en que piensa utilizar AWS Config.

Paso 1: ejecución de put-configuration-recorder

Utilice el comando `put-configuration-recorder` para crear un registrador de configuración administrado por el cliente:

Este comando usa los campos `--configuration-recorder` y `---recording-group`.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

El campo **`configuration-recorder`**

El archivo `configurationRecorder.json` especifica el `name` y el `roleArn`, además de la frecuencia de registro predeterminada para el registro de la configuración (`recordingMode`). También puede usar este campo para anular la frecuencia de registro de tipos de recursos específicos.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

El campo **`recording-group`**

El campo `recordingGroup.json` especifica los tipos de recursos que se registran.

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
```

```
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

Para obtener más información acerca de estos campos, consulte `put-configuration-recorder` en la Referencia de comandos de la AWS CLI.

Paso 2: ejecutar el comando put-delivery-channel

Utilice el comando `put-delivery-channel` para crear un canal de entrega:

Este comando usa el campo `--delivery-channel`.

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

El campo **`delivery-channel`**

El archivo `deliveryChannel.json` especifica lo siguiente:

- El `name` del canal de entrega.
- El `s3BucketName` donde AWS Config envía las instantáneas de configuración.
- El `snsTopicARN` donde AWS Config envía las notificaciones
- `configSnapshotDeliveryProperties` que establece la frecuencia con la que AWS Config entrega instantáneas de configuración y con la que invoca las evaluaciones de reglas periódicas.

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Para obtener más información acerca de estos campos, consulte `put-delivery-channel` en la Referencia de comandos de la AWS CLI.

Paso 3: ejecutar el comando start-configuration-recorder

Usa el comando `start-configuration-recorder` para iniciar AWS Config:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Para obtener más información acerca de estos campos, consulte `start-configuration-recorder` en la Referencia de comandos de la AWS CLI.

Verificación de que AWS Config se ha iniciado correctamente con el AWS CLI

Una vez que haya empezado AWS Config, puede utilizar AWS CLI los comandos para comprobar que AWS Config se está ejecutando y que se AWS Config ha creado un grabador de configuración y un canal de entrega. También puede confirmar que AWS Config ha empezado a grabar y entregar las configuraciones al canal de entrega.

Temas

- Paso 1: comprobación de creación del canal de entrega
- Paso 2: comprobación de creación del registrador de configuración
- Paso 3: Comprueba que se AWS Config ha iniciado la grabación

Paso 1: comprobación de creación del canal de entrega

Utilice el comando `describe-delivery-channels` para verificar que se hayan configurado el bucket de Amazon S3 y el tema de Amazon SNS.

Puede usar el campo `--delivery-channel-names` para especificar una lista de canales de entrega. Si no se especifica ningún canal de entrega, este comando devuelve los detalles de todos los canales de entrega asociados a la cuenta.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

Paso 2: comprobación de creación del registrador de configuración

Utilice el comando `describe-configuration-recorders` para comprobar que se ha creado un registrador de configuración.

Puede usar los campos `arn` y `configuration-recorder-names` para especificar una lista de registradores de configuración. Si no se especifica ningún registrador de configuración, este comando devuelve los detalles de todos los registradores de configuración asociados a la cuenta.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Paso 3: Comprueba que se AWS Config ha iniciado la grabación

Utilice el comando `describe-configuration-recorder-status` para comprobar que el registrador de configuración registra correctamente los tipos de recursos incluidos en el ámbito.

Puede usar los campos `arn` y `configuration-recorder-names` para especificar una lista de registradores de configuración. Si no se especifica ningún registrador de configuración, este comando devuelve los detalles de todos los registradores de configuración asociados a la cuenta.

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
```

```
    ]
}
```

El valor `true` del campo `recording` confirma que el registrador de configuración ha comenzado a registrar las configuraciones. AWS Config registra la hora en UTC. El resultado se muestra como una marca temporal de Unix.

AWS Config Utilizándolo con un AWS SDK

AWS Los kits de desarrollo de software (SDKs) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK para C++	AWS SDK para C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK para Go	AWS SDK para Go ejemplos de código
AWS SDK para Java	AWS SDK para Java ejemplos de código
AWS SDK para JavaScript	AWS SDK para JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código
AWS SDK para .NET	AWS SDK para .NET ejemplos de código
AWS SDK para PHP	AWS SDK para PHP ejemplos de código
Herramientas de AWS para PowerShell	Herramientas de AWS para PowerShell ejemplos de código
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) ejemplos de código
AWS SDK para Ruby	AWS SDK para Ruby ejemplos de código
AWS SDK para Rust	AWS SDK para Rust ejemplos de código

Documentación de SDK	Ejemplos de código
AWS SDK para SAP ABAP	AWS SDK para SAP ABAP ejemplos de código
AWS SDK para Swift	AWS SDK para Swift ejemplos de código

Ejemplo de disponibilidad

¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Uso del registrador de configuración

El grabador de configuración almacena los cambios de configuración en los tipos de recursos incluidos en el ámbito como elementos de configuración (CIs).

Existen dos tipos de registradores de configuración.

Tipo	Descripción
Registrador de configuración administrado por el cliente	Un registrador de configuración que administr a usted. Usted establece los tipos de recursos incluidos en el ámbito. De forma predeterm inada, un grabador de configuración administr ado por el cliente registra todos los recursos compatibles en el Región de AWS lugar donde AWS Config se están ejecutando.
Registrador de configuración vinculado a servicios	Un grabador de configuración que está vinculado a un registro específico Servicio de AWS. Los tipos de recursos incluidos en el ámbito los establece el servicio vinculado.

Temas

- Consideraciones sobre el registrador de configuración administrado por el cliente
- Consideraciones sobre los registradores de configuración vinculados a servicios
- Detección de desviaciones para el registrador de configuración
- Inicio del registrador de configuración administrado por el cliente
- Detención del registrador de configuración administrado por el cliente
- Cambio de la frecuencia de registro del registrador de configuración administrado por el cliente
- Cambio del nombre del registrador de configuración administrado por el cliente
- Visualización de los registradores de configuración
- Eliminación de registradores de configuración

Consideraciones sobre el registrador de configuración administrado por el cliente

Un registrador de configuración administrado por el cliente por cuenta y región

Solo puede tener un grabador de configuración administrado por el cliente Cuenta de AWS para cada uno Región de AWS.

El valor predeterminado es registrar todos los tipos de recursos admitidos, excepto los tipos de recursos de IAM globales

El valor predeterminado de un registrador de configuración administrado por el cliente es registrar todos los tipos de recursos admitidos, excepto los siguientes tipos de recursos de IAM globales: `AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role` y `AWS::IAM::User`. Puede especificar qué tipos de recursos desea incluir o excluir del registro.

Para obtener más información, consulte Grabación de AWS recursos con AWS Config.

Se le cobrarán las tarifas de uso del servicio del registrador de configuración administrado por el cliente

Se le cobrarán tarifas de uso del servicio cuando AWS Config comience a grabar las configuraciones con el grabador de configuraciones administrado por el cliente.

Para obtener información acerca de los precios, consulte Precios de AWS Config.

Se utiliza AWS Systems Manager para crear un grabador de configuración gestionado por el cliente en toda la organización

Puedes usar AWS Systems Manager Quick Setup para crear un registrador de configuración gestionado por el cliente en varias unidades organizativas (OUs) y Regiones de AWS siguiendo las prácticas AWS recomendadas.

Para obtener más información, consulte Creación de un grabador de AWS Config configuración mediante Quick Setup en la Guía del usuario de Systems Manager.

> **Important**
>
> Políticas y resultados de cumplimiento

Las políticas de IAM y otras políticas gestionadas AWS Organizations pueden afectar a la disponibilidad AWS Config de permisos para registrar los cambios de configuración de sus recursos. Además, las reglas evalúan directamente la configuración de un recurso y no tienen en cuenta estas políticas al ejecutar las evaluaciones. Asegúrese de que las políticas en vigor se ajusten a la forma en que piensa utilizar AWS Config.

Los resultados de la evaluación de los recursos obsoletos pueden persistir si el registrador de configuración está desactivado

Si el registrador de configuración administrado por el cliente está desactivado, se deshabilita la posibilidad de que AWS Config Config realice un seguimiento de los cambios en la configuración de los recursos, incluida su eliminación. Esto significa que es posible que vea resultados de evaluación obsoletos de los recursos que se eliminan cuando el registrador de configuración administrado por el cliente está apagado, ya que AWS Config no puede capturar los eventos de eliminación si el registro no está activado.

Consideraciones sobre los registradores de configuración vinculados a servicios

Se debe AWS Config utilizar la función vinculada al servicio

El rol AWS Config vinculado al servicio es obligatorio para los grabadores de configuración vinculados al servicio.

Para obtener más información, consulte Uso de roles vinculados a servicios para AWS Config.

Los registradores de configuración vinculados a servicios siempre registran

Los registradores vinculados a servicios son fijos. No puede cambiar directamente la configuración de un registrador vinculado a servicios. Para modificar la configuración de la grabadora, como iniciar, detener o actualizar la grabadora, realice estos cambios a través del AWS servicio asociado que utiliza la grabadora vinculada al servicio.

Para obtener más información, consulte Eliminación del registrador de configuración.

El ámbito de registro determina si recibe elementos de configuración

El alcance del registro lo establece el Servicio de AWS que está vinculado a la grabadora de configuración y determina si se reciben los elementos de configuración (CIs) en el canal de entrega. Si el ámbito de grabación es INTERNO, no lo recibirá CIs en el canal de entrega.

El ámbito de registro determina si se le cobra una tarifa de servicio

El alcance del registro lo establece el Servicio de AWS que está vinculado al registrador de configuración y determina si los elementos de configuración (CIs) incluidos en el alcance se graban de forma gratuita (INTERNO) o si esto repercute en los costes de la factura (PAGADO).

Prioridad de frecuencia de registro entre registradores

Si tiene un registrador de configuración administrado por el cliente y un registrador de configuración vinculado a servicios con un ámbito de registro de “DE PAGO” que registra los mismos tipos de recursos, tiene prioridad el registrador con la frecuencia de registro más alta. Por ejemplo, si su grabadora gestionada por el cliente está configurada para la grabación diaria, pero usted habilita un AWS servicio que utiliza una grabadora vinculada a un servicio con un alcance de grabación «de pago» y grabación continua, los tipos de recursos afectados se grabarán de forma continua.

Esto significa que, aunque la configuración del registrador administrado por el cliente siga mostrando “Registro diario”, se le cobrará por el registro continuo para los tipos de recursos disponibles para ambos registradores. Esto solo afecta a los tipos de recursos que registran ambos registradores.

> **Note**
>
> Solo se le cobrará una vez por elemento de configuración, independientemente del número de elementos de configuración generados por un registrador de configuración administrado por el cliente o por los registradores de configuración vinculados a servicios que pague.

Example Ejemplo: prioridad de frecuencia de registro

Ha configurado su registrador administrado por el cliente para registrar instancias de Amazon EC2 con una frecuencia de registro diario. Más adelante, habilita una función de AWS servicio que utiliza una grabadora vinculada a un servicio con un alcance de grabación de «PAID» y una grabación continua que también graba instancias de Amazon EC2. En este escenario:

- La configuración del registrador administrado por el cliente seguirá mostrando “Registro diario”
- Las instancias Amazon EC2 se graban de forma continua y proporcionan más, CIs ya que la grabadora vinculada al servicio con un alcance de grabación de «PAID» tiene una frecuencia de grabación más alta.
- Se le cobrará por el registro continuo de las instancias de Amazon EC2

- Otros tipos de recursos que solo administra su registrador administrado por el cliente seguirán registrándose con frecuencia diaria

Servicios admitidos

Los registradores de configuración vinculados a servicios son compatibles con los siguientes servicios:

AWS service	Entidad principal de servicio	Ventajas de usarlo con AWS Config	Más información
Amazon CloudWatch	`observabilityadmin.amazonaws.com`, `telemetry-enablement.observabilityadmin.amazonaws.com`	Puede utilizar Amazon CloudWatch Observability Admin para descubrir y comprender el estado de la configuración de telemetría de su AWS organización o cuenta. CloudWatch	Para obtener más información, consulte Auditar las configuraciones de CloudWatch telemetría en la Guía del usuario. CloudWatch
AWS Security Hub CSPM	`securityhub.amazonaws.com`	Puede utilizarla AWS Security Hub CSPM para gestionar de forma centralizada las conclusiones de seguridad y realizar evaluaciones de seguridad en todas sus AWS cuentas. El registrador vinculado a servicios permite utilizar un enfoque basado en eventos para obtener los elementos de	Para obtener más información, consulte Habilitar Security Hub en la Guía del usuario de Security Hub CSPM.

AWS service	Entidad principal de servicio	Ventajas de usarlo con AWS Config	Más información
		configuración de los recursos necesario s para la cobertura del análisis de la exposición.	

Detección de desviaciones para el registrador de configuración

El tipo de recurso `AWS::Config::ConfigurationRecorder` es un elemento de configuración (CI, por sus siglas en inglés) para el registrador de configuración que realiza el seguimiento de todos los cambios del estado del registrador de configuración. Puede usar este CI para comprobar si el estado del registrador de configuración es diferente o se ha desviado del estado anterior.

Por ejemplo, este CI registra si hay actualizaciones en los tipos de recursos que ha permitido que siga AWS Config , si ha detenido o iniciado el registrador de configuración o si ha eliminado o desinstalado el registrador de configuración. Un registrador de configuración desviado indica que no está detectando con precisión los cambios en los tipos de recursos previstos. Si el registrador de configuración está desviado, es posible que los resultados de conformidad sean falsos negativos o falsos positivos.

El tipo de `AWS::Config::ConfigurationRecorder` recurso es un tipo de recurso del sistema AWS Config y el registro de este tipo de recurso está habilitado de forma predeterminada en todas las regiones compatibles. El registro de este tipo de recurso `AWS::Config::ConfigurationRecorder` no tiene costo adicional.

Inicio del registrador de configuración administrado por el cliente

Puede utilizar la AWS Config consola o AWS CLI iniciar el grabador de configuración gestionado por el cliente.

To start the customer managed configuration recorder (Console)

1. Inicie sesión en la AWS Config consola Consola de administración de AWS y ábrala en https://console.aws.amazon.com/config/casa.
2. Seleccione Configuración en el panel de navegación.

3. En la pestaña Registrador administrado por el cliente, seleccione Iniciar registro. Cuando se le pida confirmación, elija Confirmar.

To start the customer managed configuration recorder (CLI)

Utilice el comando `start-configuration-recorder`:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Detención del registrador de configuración administrado por el cliente

> **Note**
>
> Los registradores de configuración vinculados a servicios siempre registran
> No se puede detener un registrador de configuración vinculado a servicios porque los registradores de configuración vinculados a servicios siempre están grabando. Para detener la registro, debe eliminar el registrador de configuración vinculado a servicios. Para obtener más información, consulte Eliminación del registrador de configuración.

Puede utilizar la AWS Config consola o AWS CLI detener el grabador de configuración gestionado por el cliente.

To stop the customer managed configuration recorder (Console)

1. Inicie sesión en la AWS Config consola Consola de administración de AWS y ábrala en https://console.aws.amazon.com/config/casa.
2. Seleccione Configuración en el panel de navegación.
3. En la pestaña Registrador administrado por el cliente, seleccione Detener registro. Cuando se le pida confirmación, elija Confirmar.

To stop the customer managed configuration recorder (CLI)

Utilice el comando `stop-configuration-recorder`:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

Cambio de la frecuencia de registro del registrador de configuración administrado por el cliente

AWS Config admite la grabación continua y la grabación diaria:

- El registro continuo permite registrar los cambios de configuración de forma continua siempre que se produzca un cambio.
- El registro diario permite recibir un elemento de configuración (CI) que representa el estado más reciente de los recursos durante el último período de 24 horas, solo si es diferente del CI anterior registrado. Para obtener más información, consulte Frecuencia de registro.

Puede utilizar la AWS Config consola o AWS CLI cambiar la frecuencia de grabación.

To change the recording frequency for the customer managed configuration recorder (Console)

1. Inicie sesión en la AWS Config consola Consola de administración de AWS y ábrala en https://console.aws.amazon.com/config/casa.
2. Seleccione Configuración en el panel de navegación.
3. En la pestaña Registrador administrado por el cliente, seleccione Iniciar registro.
4. En Registrador administrado por método de registro, seleccione Todos los tipos de recursos con anulaciones personalizables.
5. En Configuración predeterminada, elija una frecuencia de registro.
6. Seleccione Save.

To change the recording frequency (CLI)

Utilice el comando `put-configuration-recorder` para cambiar la frecuencia de registro del registro de configuración:

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

El archivo `configurationRecorder.json` especifica el `name` y el `roleArn`, además de la frecuencia de registro predeterminada para el registro de la configuración (`recordingMode`). También puede usar este campo para anular la frecuencia de registro de tipos de recursos específicos.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

`put-configuration-recorder` utiliza los siguientes campos para el parámetro `--configuration-recorder`:

- `name`: el nombre del registrador de la configuración; AWS Config asigna automáticamente el nombre predeterminado al crear el registrador de configuración.
- `roleARN`— Nombre de recurso de Amazon (ARN) de la función de IAM que asume AWS Config y utiliza el grabador de configuración.
- `recordingMode`— Especifica la frecuencia de grabación predeterminada que se AWS Config utiliza para registrar los cambios de configuración. AWS Config admite la grabación continua y la grabación diaria. El registro continuo permite registrar los cambios de configuración de forma continua siempre que se produzca un cambio. El registro diario permite recibir un elemento de configuración (CI) que representa el estado más reciente de los recursos durante el último período de 24 horas, solo si es diferente del CI anterior registrado.
  - `recordingFrequency`— La frecuencia de grabación predeterminada que se AWS Config utiliza para registrar los cambios de configuración.

> **Note**
>
> AWS Firewall Manager depende de la grabación continua para monitorizar sus recursos. Si utiliza Firewall Manager, se recomienda configurar la frecuencia de registro en Continua.

- `recordingModeOverrides`: este campo le permite especificar las anulaciones para el modo de registro. Es una matriz de objetos de `recordingModeOverride`. Cada objeto `recordingModeOverride` de la matriz `recordingModeOverrides` consta de tres campos:
  - `description`: la descripción que proporcione para la anulación.
  - `recordingFrequency`: la frecuencia de registro que se aplicará a todos los tipos de recursos especificados en la anulación.
  - `resourceTypes`— Una lista separada por comas que especifica qué tipos de recursos se AWS Config incluyen en la anulación.

> **Note**
>
> Campos obligatorios y opcionales
>
> El campo `recordingMode` de `put-configuration-recorder` es opcional. De forma predeterminada, la frecuencia de registro del registro de configuración está definida como Registro continuo.

> **Note**
>
> Límites
>
> No se admite la grabación diaria para los siguientes tipos de recursos:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Para la estrategia de registro Registrar todos los tipos de recursos compatibles actuales y futuros (`ALL_SUPPORTED_RESOURCE_TYPES`), estos tipos de recursos se definirán con Registro continuo.

Cambio del nombre del registrador de configuración administrado por el cliente

Debe utilizarla AWS CLI para cambiar el nombre del grabador de configuración gestionado por el cliente. Para cambiar el nombre del registrador de configuración administrado por el cliente, debe eliminarlo y crear un nuevo registrador de configuración con el nombre especificado.

Cambiar el nombre del grabador de configuración gestionado por el cliente mediante el AWS CLI

1. Utilice el comando `describe-configuration-recorders` para buscar el nombre del registrador de configuración actual administrado por el cliente:

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

2. Utilice el comando `delete-configuration-recorder` para eliminar el registrador de configuración actual administrado por el cliente:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. Utilice el comando `put-configuration-recorder` para crear un registrador de configuración administrado por el cliente con el nuevo nombre:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. Utilice el comando `start-configuration-recorder` para reanudar el registro:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Visualización de los registradores de configuración

Puede utilizar la consola de AWS Config o la AWS CLI para ver detalles de los registradores de configuración.

To view your configuration recorders (Console)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Config en https://console.aws.amazon.com/config/home.
2. Seleccione Configuración en el panel de navegación.
3. Para el registrador de configuración administrado por el cliente, puede ver los detalles en la pestaña Registrador administrado por el cliente.
4. Para registradores de configuración vinculados a servicios, seleccione un registrador de configuración vinculado a servicios en la pestaña Registradores vinculados a servicios y, a continuación, seleccione Ver.

To view your configuration recorders (CLI)

Utilice el comando `describe-configuration-recorders` para ver detalles sobre sus registradores de configuración:

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Utilice el comando `describe-configuration-recorder-status` para ver el estado actual de sus registradores de configuración:

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

Para estos dos comandos, puede usar los campos `arn` y `configuration-recorder-names` para especificar una lista de registradores de configuración. En el caso de los registradores de configuración vinculados a servicios, puede utilizar el campo `service-principal` para especificar un registrador de configuración.

Si no se especifica ningún registrador de configuración, este comando devuelve los detalles de todos los registradores de configuración asociados a la cuenta.

Eliminación de registradores de configuración

Debe utilizar el AWS CLI para eliminar el grabador de configuración gestionado por el cliente. Puede usar la AWS Config consola o la AWS CLI para eliminar un grabador de configuración vinculado a un servicio.

To delete the customer managed configuration recorder (CLI)

Utilice el comando `delete-configuration-recorder`:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To delete a service-linked configuration recorder (Console)

1. Inicie sesión en la AWS Config consola Consola de administración de AWS y ábrala en https://console.aws.amazon.com/config/ casa.
2. Seleccione Configuración en el panel de navegación.
3. En la pestaña Registradores de configuración vinculados a servicios, seleccione un registrador de configuración vinculado a servicios en la pestaña Registradores vinculados a servicios y, a continuación, seleccione Eliminar. Cuando se le pregunte, elija Delete (Eliminar).

To delete a service-linked configuration recorder (CLI)

Utilice el comando `delete-service-linked-configuration-recorder`:

Este comando usa el campo `--service-principal`.

```
$ aws configservice delete-service-linked-configuration-recorder --service-principal
 "The service principal of the Servicio de AWS for the service-linked configuration
 recorder that you want to delete"
```

Trabajo con el canal de entrega

Como registra AWS Config continuamente los cambios que se producen en sus AWS recursos, envía notificaciones y estados de configuración actualizados a través del canal de entrega. Puede administrar el canal de entrega para controlar dónde se AWS Config envían las actualizaciones de configuración.

Temas

- Consideraciones
- Terminología
- Componentes de un elemento de configuración
- Visualización del canal de entrega
- Actualización del canal de entrega
- Cambio de nombre del canal de entrega
- Entrega de instantáneas de configuración a un bucket de Amazon S3
- Verificación del estado de entrega
- Visualización de las instantáneas de la configuración en el bucket de Amazon S3
- Ejemplo de instantánea de configuración de AWS Config
- Notificaciones que se AWS Config envían a un tema de Amazon SNS

Consideraciones

Un canal de entrega por región y por cuenta

Solo puede tener un canal de entrega por AWS región y región Cuenta de AWS, y es obligatorio utilizar el canal de entrega AWS Config.

Las notificaciones de elementos de configuración sobredimensionados incluyen un breve resumen

Cuando AWS Config detecta un cambio en la configuración de un recurso y la notificación supera el tamaño máximo permitido por Amazon SNS, la notificación incluye un breve resumen del elemento de configuración. Puede ver la notificación completa en la ubicación del bucket de Amazon S3 especificada en el campo `s3BucketLocation`. Para obtener más información, consulte Example Oversized Configuration Item Change Notification.

AWS Config admite el AWS KMS cifrado de los buckets de Amazon S3 utilizados por AWS Config

Puede proporcionar una clave AWS Key Management Service (AWS KMS) o un alias (Amazon Resource Name, ARN) para cifrar los datos que se envían a su bucket de Amazon Simple Storage Service (Amazon S3). De forma predeterminada, AWS Config entrega el historial de configuración y los archivos de instantáneas a su bucket de Amazon S3 y cifra los datos en reposo mediante el cifrado S3 AES-256 del lado del servidor, SSE-S3. Sin embargo, si AWS Config proporciona su clave de KMS o alias ARN, AWS Config utiliza esa clave de KMS en lugar del cifrado AES-256.

AWS Config no admite el canal de entrega a un bucket de Amazon S3 en el que el bloqueo de objetos está habilitado con la retención predeterminada habilitada. Para obtener más información, consulte Cómo funciona el bloqueo de objetos de S3.

Terminología

Un elemento de configuración representa una point-in-time vista de los distintos atributos de un AWS recurso compatible que existe en su cuenta. Los componentes de un elemento de configuración incluyen los metadatos, los atributos, las relaciones, la configuración actual y los eventos relacionados. AWS Config crea un elemento de configuración cada vez que detecta un cambio en un tipo de recurso que está registrando. Por ejemplo, si AWS Config está grabando buckets de Amazon S3, AWS Config crea un elemento de configuración cada vez que se crea, actualiza o elimina un bucket. También puede seleccionar AWS Config crear un elemento de configuración con la frecuencia de grabación que haya establecido.

Un historial de configuración es una colección de elementos de configuración de un recurso determinado durante cualquier periodo de tiempo. Un historial de configuración puede ayudarle a responder preguntas sobre, por ejemplo, cuándo se creó el recurso, cómo se ha configurado durante el último mes y qué cambios de configuración se introdujeron ayer a las 9 de la mañana. El historial de configuración está disponible en varios formatos. AWS Config entrega automáticamente un archivo de historial de configuración para cada tipo de recurso que se registre en un bucket de Amazon S3 que especifique. Puede seleccionar un recurso determinado en la AWS Config consola y navegar hasta todos los elementos de configuración anteriores de ese recurso utilizando la cronología. Asimismo, puede obtener acceso a los elementos de configuración históricos de un recurso desde la API.

Una instantánea de configuración es una colección de elementos de configuración de los recursos admitidos que existen en su cuenta. Esta instantánea de configuración es una imagen completa de los recursos que se registran y sus configuraciones. La instantánea de configuración puede ser una herramienta útil para validar la configuración. Por ejemplo, puede examinar la instantánea de

configuración con regularidad para los recursos que se han configurado de forma incorrecta o que potencialmente no deban existir. La instantánea de configuración está disponible en varios formatos. Puede hacer que la instantánea de configuración se entregue al bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Además, puede seleccionar un punto en el tiempo en la AWS Config consola y navegar por la instantánea de los elementos de configuración utilizando las relaciones entre los recursos.

Un flujo de configuración es una lista que se actualiza automáticamente de todos los elementos de configuración de los recursos que AWS Config se están registrando. Cada vez que se crea, se modifica o se elimina un recurso, AWS Config crea un elemento de configuración y lo añade al flujo de configuración. El flujo de configuración utiliza el tema de Amazon Simple Notification Service (Amazon SNS) de su elección. El flujo de configuración es útil para observar los cambios de configuración a medida que se producen y detectar posibles problemas, generar notificaciones si se modifican determinados recursos o actualizar los sistemas externos que deben reflejar la configuración de AWS los recursos.

Componentes de un elemento de configuración

Un elemento de configuración representa una vista en un punto en el tiempo de los diversos atributos de un recurso de AWS admitido que existe en su cuenta. Los componentes de un elemento de configuración incluyen metadatos, atributos, relaciones, la configuración actual y eventos relacionados. AWS Config crea un elemento de configuración cuando se detecta un cambio en un tipo de recurso que se está registrando. Por ejemplo, si AWS Config está registrando buckets de Amazon S3, AWS Config crea un elemento de configuración siempre que se crea, actualiza o elimina un bucket. También puede seleccionar que AWS Config cree un elemento de configuración con la frecuencia de registro que haya establecido.

Un elemento de configuración consta de los siguientes componentes.

Componente	Descripción	Contiene
Metadatos	Información sobre este elemento de configuración.	• ID de versión. • Hora en la que se ha capturado el elemento de configuración. • Estado del elemento de configuración que indica si el elemento se ha capturado correctamente.

Componente	Descripción	Contiene
		• ID de estado que indica la ordenación de los elementos de configuración de un recurso.
Atributos	Atributos de recursos	• ID de recursos • Lista de etiquetas clave-valor de este recurso • Tipo de recurso (consulte Tipos de recursos compatibles para AWS Config) • nombre de recurso de Amazon (ARN) • Zona de disponibilidad que contiene este recurso, si procede • Hora a la que se ha creado el recurso
Relaciones	Cómo se relaciona el recurso con otros recursos asociados a la cuenta	Descripción de la relación, por ejemplo, el volumen de Amazon EBS `vol-1234567` vinculado a una instancia `i-a1b2c3d4` de Amazon EC2

Componente	Descripción	Contiene
Configuración actual	La información que se devuelve a través de una llamada a las API Describe o List del recurso	Por ejemplo, la API `DescribeVolumes` devuelve la siguiente información sobre el volumen: • Zona de disponibilidad en la que se encuentra el volumen • Hora a la que se ha conectado el volumen • ID de la instancia EC2 a la que está conectado • Estado actual del volumen • Estado de la marca DeleteOnTermination • Dispositivo al que está conectado el volumen • Tipo de volumen, como por ejemplo `gp2`, `io1`, o `standard`

Notas

1. La relación de un elemento de configuración no incluye el flujo de red o las dependencias de flujo de datos. Los elementos de configuración no se puede personalizar para representar la arquitectura de su aplicación.
2. A partir de la versión 1.3, el campo relatedEvents está vacío. Puede acceder a la API LookupEvents en la Referencia de la API de AWS CloudTrail para obtener los eventos para el recurso.
3. A partir de la versión 1.3, el campo configurationItemMD5Hash está vacío. Puede utilizar el campo configurationStateId para asegurarse de que dispone del elemento de configuración más reciente.
4. Si un tipo de recurso no admite etiquetado o no incluye información sobre etiquetas en la respuesta de descripción de la API, AWS Config no capturará datos de las etiquetas en los elementos de configuración (CI) para ese tipo de recurso. AWS Config seguirá registrando estos recursos. Sin embargo, cualquier funcionalidad que dependa de los datos de las etiquetas no funcionará. Esto afecta al filtrado, la agrupación o la evaluación del cumplimiento que se basan en los datos de las etiquetas.

Visualización del canal de entrega

Debe utilizar el AWS CLI para ver los detalles del canal de entrega.

Los siguientes ejemplos de código muestran cómo utilizar `DescribeDeliveryChannels`.

CLI

AWS CLI

Información sobre el canal de entrega

El comando siguiente devuelve información detallada sobre el canal de entrega:

```
aws configservice describe-delivery-channels
```

Salida:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeDeliveryChannelsla Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se recupera el canal de entrega de la región y se muestran los detalles.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Salida:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Para obtener más información sobre la API, consulte DescribeDeliveryChannels Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se recupera el canal de entrega de la región y se muestran los detalles.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Salida:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Para obtener más información sobre la API, consulte DescribeDeliveryChannelsla referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Actualización del canal de entrega

Al actualizar el canal de entrega, puede ajustar las siguientes opciones:

- El bucket de Amazon S3 desde el que se AWS Config envían las instantáneas de la configuración y los archivos del historial de configuración.
- Con qué frecuencia AWS Config entrega instantáneas de configuración a su bucket de Amazon S3.
- El tema de Amazon SNS al que se AWS Config envían notificaciones sobre los cambios de configuración.

Actualización del canal de entrega (consola)

Puede usar la AWS Config consola para configurar el bucket de Amazon S3 y el tema Amazon SNS para su canal de entrega. Para conocer los pasos para administrar estos ajustes, consulte Configuración de AWS Config con la consola.

La consola no proporciona opciones para cambiar el nombre del canal de entrega, ajustar la frecuencia de las instantáneas de configuración o eliminar el canal de entrega. Para realizar estas tareas, debe utilizar la AWS CLI, la AWS Config API o una de las AWS SDKs.

Para actualizar el canal de entrega (AWS SDKs)

Los siguientes ejemplos de código muestran cómo utilizar `PutDeliveryChannel`.

CLI

AWS CLI

Creación de un canal de entrega

El siguiente comando proporciona la configuración del canal de entrega en forma de código JSON:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

El archivo `deliveryChannel.json` especifica los atributos del canal de entrega:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Este ejemplo establece los siguientes atributos:

`name`: El nombre del canal de entrega. De forma predeterminada, AWS Config asigna el nombre `default` a un nuevo canal de entrega. No puede actualizar el nombre del canal de entrega con el comando. `put-delivery-channel` Si desea saber cuáles son los

pasos para cambiar el nombre, consulte Renaming the Delivery Channel. `s3BucketName`: - El nombre del bucket de Amazon S3 al que AWS Config entrega las instantáneas de configuración y los archivos del historial de configuración. Si especifica un bucket que pertenece a otra AWS cuenta, ese bucket debe tener políticas que concedan permisos de acceso a Config. AWS Para obtener más información, consulte Permisos para el bucket de Amazon S3.

`snsTopicARN`- El nombre del recurso de Amazon (ARN) del tema de Amazon SNS al que AWS Config envía notificaciones sobre los cambios de configuración. Si elige un tema de otra cuenta, el tema debe tener políticas que concedan permisos de acceso a Config. AWS Para obtener más información, consulte Permissions for the Amazon SNS Topic.

`configSnapshotDeliveryProperties`- Contiene el `deliveryFrequency` atributo, que establece la frecuencia con la que AWS Config entrega instantáneas de la configuración y la frecuencia con la que invoca las evaluaciones de las reglas de Config periódicas.

Si el comando se ejecuta correctamente, AWS Config no devuelve ningún resultado. Para verificar la configuración de su canal de entrega, ejecute el describe-delivery-channels comando.

- Para obtener más información sobre la API, consulte PutDeliveryChannella Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se cambia la propiedad deliveryFrequency de un canal de entrega existente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- Para obtener más información sobre la API, consulte PutDeliveryChannel Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se cambia la propiedad deliveryFrequency de un canal de entrega existente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- Para obtener más información sobre la API, consulte PutDeliveryChannella referencia de Herramientas de AWS para PowerShell cmdlets (V5).

(Opcional) Puede utilizar el comando `describe-delivery-channels` para verificar que se han actualizado los ajustes del canal de entrega:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

Los siguientes ejemplos de código muestran cómo utilizar `DescribeDeliveryChannels`.

CLI

AWS CLI

Información sobre el canal de entrega

El comando siguiente devuelve información detallada sobre el canal de entrega:

```
aws configservice describe-delivery-channels
```

Salida:

```
{
    "DeliveryChannels": [
```

```
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte la Referencia de DescribeDeliveryChannelscomandos AWS CLI .

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se recupera el canal de entrega de la región y se muestran los detalles.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Salida:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Para obtener más información sobre la API, consulte DescribeDeliveryChannels Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se recupera el canal de entrega de la región y se muestran los detalles.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Salida:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Para obtener más información sobre la API, consulte DescribeDeliveryChannelsla referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Cambio de nombre del canal de entrega

Para cambiar el nombre del canal de entrega, debe eliminarlo y crear un nuevo canal de entrega con el nombre que desee. Antes de poder eliminar el canal de entrega, debe detener temporalmente el registrador de configuración. La AWS Config consola no ofrece la opción de eliminar el canal de entrega. Debe usar la AWS CLI, la AWS Config API o una de las AWS SDKs.

Cambiar el nombre del canal de entrega mediante AWS CLI

1. Utilice el comando `stop-configuration-recorder` para detener el registrador de configuración:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. Utilice el comando `describe-delivery-channels` y anote los atributos de su canal de entrega:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. Utilice el comando `delete-delivery-channel` para eliminar el canal de entrega:

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Utilice el comando `put-delivery-channel` para crear un canal de entrega con el nombre que desee:

```
$ aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

El archivo deliveryChannel.json especifica los atributos del canal de entrega:

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. Utilice el comando `start-configuration-recorder` para reanudar el registro:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Entrega de instantáneas de configuración a un bucket de Amazon S3

Una instantánea de configuración es una colección de elementos de configuración de los recursos admitidos que existen en su cuenta. Esta instantánea de configuración es una imagen completa de los recursos que se registran y sus configuraciones. La instantánea de configuración puede ser una herramienta útil para validar la configuración. Por ejemplo, puede examinar la instantánea de configuración con regularidad para los recursos que se han configurado de forma incorrecta o que potencialmente no deban existir. La instantánea de configuración está disponible en varios formatos. Puede hacer que la instantánea de configuración se entregue al bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Además, puede seleccionar un punto en el tiempo en la AWS Config consola y navegar por la instantánea de los elementos de configuración utilizando las relaciones entre los recursos.

Entrega de instantáneas de configuración

AWS Config genera instantáneas de configuración cuando se invoca la DeliverConfigSnapshotacción o se ejecuta el AWS CLI `deliver-config-snapshot` comando. AWS Config almacena las instantáneas de configuración en el bucket de Amazon S3 que especificó al AWS Config habilitarlo.

Introduzca el `deliver-config-snapshot`comando especificando el nombre asignado AWS Config al configurar el canal de entrega, por ejemplo:

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

Verificación del estado de entrega

Introduzca el `describe-delivery-channel-status`comando para comprobar que AWS Config ha empezado a entregar las configuraciones al canal de entrega especificado:

```
aws configservice describe-delivery-channel-status
```

La respuesta muestra el estado de los tres formatos de entrega que se AWS Config utilizan para entregar las configuraciones al segmento y al tema.

```
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
```

```
            },
            "name": "default"
        }
    ]
}
```

Vea el campo `lastSuccessfulTime` en `configSnapshotDeliveryInfo`. La hora debe coincidir con la hora a la que solicitó por última vez la entrega de la instantánea de la configuración.

> **Note**
>
> AWS Config utiliza el formato UTC (hora universal coordinada) para registrar la hora.

Visualización de las instantáneas de la configuración en el bucket de Amazon S3

Una instantánea de configuración es una colección de elementos de configuración de los recursos admitidos que existen en su cuenta. Esta instantánea de configuración es una imagen completa de los recursos que se registran y sus configuraciones. La instantánea de configuración puede ser una herramienta útil para validar la configuración. Por ejemplo, puede examinar la instantánea de configuración con regularidad para los recursos que se han configurado de forma incorrecta o que potencialmente no deban existir. La instantánea de configuración está disponible en varios formatos. Puede hacer que la instantánea de configuración se entregue al bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Además, puede seleccionar un punto en el tiempo en la AWS Config consola y navegar por la instantánea de los elementos de configuración utilizando las relaciones entre los recursos.

Visualización de instantáneas de configuración

1. Inicie sesión en la consola de Amazon S3 Consola de administración de AWS y ábrala en https://console.aws.amazon.com/s3/.
2. En la lista Todos los buckets de la consola de Amazon S3, seleccione el nombre de su bucket de Amazon S3.
3. Navegue por las carpetas anidadas del bucket hasta que vea el objeto `ConfigSnapshot` con un ID de instantánea que coincida con el ID devuelto por el comando. Descargue y abra el objeto para ver la instantánea de la configuración. El bucket de S3 también contiene un archivo

vacío llamado`ConfigWritabilityCheckFile`. AWS Config crea este archivo para comprobar que el servicio puede escribir correctamente en el bucket de S3.

Ejemplo de instantánea de configuración de AWS Config

A continuación, se muestra un ejemplo de la información que se AWS Config incluye en una instantánea de configuración. La instantánea describe la configuración de los recursos que AWS Config se están grabando en su Cuenta de AWS región actual y describe las relaciones entre estos recursos.

> **Note**
>
> La instantánea de configuración puede incluir referencias a los tipos de recursos y a los recursos IDs que no son compatibles.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
```

```
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-ce676ccc",
            "size": 1,
            "snapshotId": "",
            "availabilityZone": "us-west-2b",
            "state": "in-use",
            "createTime": "2014-02-27T21:43:53.0885+0000",
            "attachments": [
                {
                    "volumeId": "vol-ce676ccc",
                    "instanceId": "i-344c463d",
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "i-344c463d",
        "accountId": "12345678910",
        "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
        "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
        "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adb69edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a04ad92281"
```

```
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
```

```
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
```

```
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
```

```
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

El siguiente paso consiste en verificar que la instantánea de la configuración se ha entregado correctamente en el canal de entrega.

Notificaciones que se AWS Config envían a un tema de Amazon SNS

> **Note**
>
> Antes de AWS Config poder enviar notificaciones a un tema de Amazon SNS, primero debe configurar la grabadora de configuración y el canal de entrega. Para obtener más información, consulte Administración del registro de configuración y Administrar el canal de entrega.

Puede configurarlo AWS Config para transmitir los cambios de configuración y las notificaciones a un tema de Amazon SNS. Por ejemplo, cuando se actualiza un recurso, puede obtener una notificación enviada a su correo electrónico, para que pueda ver los cambios. También puede recibir una notificación cuando AWS Config evalúe sus reglas personalizadas o administradas en relación con sus recursos. Para obtener más información, consulte Inicio de sesión y supervisión. AWS Config

AWS Config envía notificaciones sobre los siguientes eventos:

- Cambio de elemento de configuración de un recurso.
- Se ha entregado el historial de configuración de un recurso a su cuenta.
- Se ha iniciado una instantánea de configuración de los recursos registrados y se ha entregado a su cuenta.
- Estado de conformidad de los recursos y si son conformes a sus reglas.
- Se ha iniciado la evaluación de una regla con respecto a los recursos.
- AWS Config no se pudo entregar la notificación a tu cuenta.

Temas

- Ejemplo de notificaciones de cambio de elemento de configuración
- Ejemplo de notificación de entrega de historial de configuración
- Ejemplo de notificación de inicio de entrega de instantánea de configuración
- Ejemplo de notificación de entrega de instantánea de configuración
- Ejemplo de notificación de cambio de conformidad
- Ejemplo de notificación de inicio de evaluación de reglas
- Ejemplo de notificación de cambio de elemento de configuración sobredimensionado
- Ejemplo de notificación de entrega fallida

Ejemplo de notificaciones de cambio de elemento de configuración

AWS Config utiliza Amazon SNS para enviar notificaciones a los puntos de conexión de las suscripciones. Estas notificaciones proporcionan el estado de entrega de las instantáneas de configuración y los historiales de configuración, y proporcionan cada elemento de configuración que se AWS Config crea cuando cambian las configuraciones de los recursos registrados. AWS AWS Config también envía notificaciones que muestran si sus recursos cumplen con sus reglas. Si opta por que las notificaciones se envíen por correo electrónico, puede utilizar filtros en su aplicación cliente de correo electrónico basados en la línea de asunto y el cuerpo del mensaje del correo electrónico.

A continuación se muestra un ejemplo de carga de una notificación de Amazon SNS que se genera cuando AWS Config detecta que el volumen de Amazon Elastic Block Store `vol-ce676ccc` está asociado a la instancia con un ID de `i-344c463d`. La notificación contiene el cambio del elemento de configuración del recurso.

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "awsAccountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
```

```
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```

Elementos de configuración para recursos con relaciones

Si un recurso está relacionado con otros recursos, un cambio en dicho recurso puede generar varios elementos de configuración. En el siguiente ejemplo, se muestra cómo AWS Config crea elementos de configuración para los recursos con relaciones.

1. Cuenta con una instancia de Amazon EC2 con un ID de `i-007d374c8912e3e90` y la instancia se asocia a un grupo de seguridad de Amazon EC2, `sg-c8b141b4`.
2. Puede actualizar la instancia EC2 para cambiar el grupo de seguridad a otro grupo de seguridad, `sg-3f1fef43`.
3. Como la instancia EC2 está relacionada con otro recurso, AWS Config crea varios elementos de configuración, como en los ejemplos siguientes:

Esta notificación contiene el cambio del elemento de configuración para la instancia EC2 cuando se sustituye el grupo de seguridad.


```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
```

```
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
```

```
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
```

```
                    "name": "Is associated with SecurityGroup"
                },
                "changeType": "CREATE"
            },
            "Configuration.SecurityGroups.1": {
                "previousValue": null,
                "updatedValue": {
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                },
                "changeType": "CREATE"
            },
            "Configuration.SecurityGroups.0": {
                "previousValue": {
                    "groupName": "example-security-group-1",
                    "groupId": "sg-c8b141b4"
                },
                "updatedValue": null,
                "changeType": "DELETE"
            }
        },
        "changeType": "UPDATE"
    },
    "configurationItem": {
        "relatedEvents": [],
        "relationships": [
            {
                "resourceId": "eni-fde9493f",
                "resourceName": null,
                "resourceType": "AWS::EC2::NetworkInterface",
                "name": "Contains NetworkInterface"
            },
            {
                "resourceId": "sg-3f1fef43",
                "resourceName": null,
                "resourceType": "AWS::EC2::SecurityGroup",
                "name": "Is associated with SecurityGroup"
            },
            {
                "resourceId": "subnet-2372be7b",
                "resourceName": null,
                "resourceType": "AWS::EC2::Subnet",
                "name": "Is contained in Subnet"
            },
```

```
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::VPC",
                    "name": "Is contained in Vpc"
                }
            ],
            "configuration": {
                "instanceId": "i-007d374c8912e3e90",
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "ec2-micro",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t2.micro",
                "launchTime": "2017-01-09T20:13:28.000Z",
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
```

```
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
```

```
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
```

```
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Esta notificación contiene el cambio del elemento de configuración para el grupo de seguridad de EC2, `sg-3f1fef43`, que está asociado a la instancia.


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
```

```
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
```

```
}
```

Comprensión del campo **`configurationItemDiff`** en las notificaciones **`ConfigurationItemChangeNotification`** de Amazon SNS

AWS Config crea un elemento de configuración cada vez que cambia la configuración de un recurso (create/update/delete). Para obtener una lista de los tipos de recursos compatibles que AWS Config se pueden registrar, consulteTipos de recursos compatibles para AWS Config. AWS Config utiliza Amazon SNS para enviar una notificación a medida que se producen los cambios. La carga útil de notificaciones de Amazon SNS incluye campos que le ayudan a realizar un seguimiento de los cambios en los recursos en una región de AWS determinada.

Para entender por qué recibe una notificación `ConfigurationItemChangeNotification`, revise los detalles de `configurationItemDiff`. Los campos varían según el tipo de cambio y pueden formar diferentes combinaciones, como UPDATE-UPDATE, UPDATE-CREATE y DELETE-DELETE. A continuación se explican algunas combinaciones comunes.

UPDATE-CREATE y UPDATE-UPDATE

El siguiente ejemplo incluye cambios en las relaciones directas de los recursos y en las configuraciones de los recursos. Los detalles de `configurationItemDiff` muestran la siguiente información:

Acción realizada: una política administrada presente en la cuenta se asoció a un rol AWS Identity and Access Management (IAM).

Operación básica realizada: UPDATE (actualización del número de asociaciones del tipo de recurso `AWS::IAM::Policy` en una cuenta).

Combinaciones de tipos de cambio:

1. Cambio de relación directa entre recursos UPDATE-CREATE. Se creó un nuevo adjunto o asociación entre una política de IAM y un rol de IAM.
2. Cambio de configuración de recursos UPDATE-UPDATE. El número de asociaciones de políticas de IAM aumentó de 2 a 3 cuando la política se asoció al rol de IAM.

Ejemplo de notificación `configurationItemDiff` UPDATE-CREATE y UPDATE-UPDATE:

```
{
```

```
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

UPDATE-DELETE

El siguiente ejemplo incluye cambios en las relaciones directas de los recursos y en las configuraciones de los recursos. Los detalles de `configurationItemDiff` muestran la siguiente información:

Acción realizada: una política administrada presente en la cuenta se desasoció de un usuario de IAM.

Operación básica realizada: UPDATE (actualización de la política de permisos asociada al tipo de recurso `AWS::IAM::User`).

Combinaciones de tipos de cambio: cambio de relación directa entre recursos (UPDATE-DELETE). Se eliminó la asociación entre un usuario de IAM y una política de IAM en una cuenta.

DELETE-DELETE

El siguiente ejemplo incluye cambios en las relaciones directas de los recursos y en las configuraciones de los recursos. Los detalles de `configurationItemDiff` muestran la siguiente información:

Acción realizada: se eliminó un rol de IAM presente en una cuenta.

Operación básica realizada: DELETE (se eliminó un recurso del tipo de recurso `AWS::IAM::Role`).

Combinaciones de tipos de cambio: cambio de relación directa del recurso y cambio de configuración del recurso DELETE-DELETE. La eliminación del rol de IAM también eliminó la asociación de la política de IAM con el rol de IAM.

Ejemplo de notificación de entrega de historial de configuración

El historial de configuración es una recopilación de elementos de configuración de un tipo de recurso a lo largo de un periodo de tiempo. El siguiente es un ejemplo de notificación que se AWS Config envía cuando se entrega el historial de configuración CloudTrail de un recurso de seguimiento a tu cuenta.


```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Ejemplo de notificación de inicio de entrega de instantánea de configuración

El siguiente es un ejemplo de notificación que se AWS Config envía cuando se AWS Config empieza a entregar la instantánea de configuración de su cuenta.


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Ejemplo de notificación de entrega de instantánea de configuración

La instantánea de configuración es una recopilación de elementos de configuración de todos los recursos registrados y de sus configuraciones en su cuenta. El siguiente es un ejemplo de notificación que se AWS Config envía cuando se entrega la instantánea de configuración de su cuenta.


```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
```

```
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Ejemplo de notificación de cambio de conformidad

Al AWS Config evaluar sus recursos con respecto a una regla personalizada o administrada, AWS Config envía una notificación que muestra si los recursos cumplen con la regla.

El siguiente es un ejemplo de notificación en el que CloudTrail el recurso de seguimiento cumple con la regla `cloudtrail-enabled` administrada.


```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
```

```
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
```

```
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Ejemplo: cambio de elemento de configuración de Config | Amazon EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
```

```
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
```

```
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

Ejemplo de notificación de inicio de evaluación de reglas

AWS Config envía una notificación cuando comienza a evaluar la regla personalizada o administrada con respecto a sus recursos. El siguiente es un ejemplo de notificación cuando AWS Config comienza a evaluar la regla `iam-password-policy` administrada.

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
```

```
}
```

Ejemplo de notificación de cambio de elemento de configuración sobredimensionado

Cuando AWS Config detecta un cambio en la configuración de un recurso, envía una notificación de elemento de configuración (CI). Si la notificación supera el tamaño máximo permitido por Amazon Simple Notification Service (Amazon SNS), la notificación incluye un breve resumen del elemento de configuración.

Puede ver la notificación completa en la ubicación del bucket de Amazon S3 especificada en el campo `s3BucketLocation`.

El siguiente ejemplo de notificación muestra un CI para una instancia de Amazon EC2. La notificación incluye un resumen de los cambios y la ubicación de la notificación en el bucket de Amazon S3.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
```

```
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "amzn-s3-demo-bucket/AWSLogs/123456789012/
Config/us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

Cómo acceder a elementos de configuración sobredimensionados

Cuando un elemento de configuración está sobredimensionado, solo se envía un resumen a Amazon SNS. El elemento de configuración (CI) completo se almacena en Amazon S3

El siguiente ejemplo de código muestra cómo acceder al CI completo.

```
import boto3
import json

def handle_oversized_configuration_item(event):
    """
    Example of handling an oversized configuration item notification

    When a configuration item is oversized:
    1. AWS Config sends a summary notification through SNS
    2. The complete configuration item is stored in S3
    3. Use get_resource_config_history API to retrieve the complete configuration
    """

    # Extract information from the summary notification
    if event['messageType'] == 'OversizedConfigurationItemChangeNotification':
        summary = event['configurationItemSummary']
        resource_type = summary['resourceType']
```

```
        resource_id = summary['resourceId']

        # Initialize AWS Config client
        config_client = boto3.client('config')

        # Retrieve the complete configuration item
        response = config_client.get_resource_config_history(
            resourceType=resource_type,
            resourceId=resource_id
        )

        if response['configurationItems']:
            config_item = response['configurationItems'][0]

            # For EC2 instances, the configuration contains instance details
            configuration = json.loads(config_item['configuration'])
            print(f"Instance Configuration: {configuration}")

            # Handle supplementary configuration if present
            if 'supplementaryConfiguration' in config_item:
                for key, value in config_item['supplementaryConfiguration'].items():
                    if isinstance(value, str):
                        config_item['supplementaryConfiguration'][key] =
json.loads(value)
                print(f"Supplementary Configuration:
{config_item['supplementaryConfiguration']}")

            return config_item

        # If needed, you can also access the complete notification from S3
        s3_location = event['s3DeliverySummary']['s3BucketLocation']
        print(f"Complete notification available in S3: {s3_location}")

    return None
```

Funcionamiento

1. La función acepta un parámetro de evento que contiene la AWS Config notificación.
2. Comprueba si el tipo de mensaje es una notificación de configuración sobredimensionada.
3. La función extrae el tipo de recurso y el ID del resumen.
4. Mediante el AWS Config cliente, recupera el historial de configuración completo.
5. La función procesa las configuraciones principales y complementarias.

6. Si es necesario, puede acceder a la notificación completa desde la ubicación de S3 proporcionada.

Ejemplo de notificación de entrega fallida

AWS Config envía una notificación de entrega fallida si no AWS Config puede entregar la instantánea de configuración o una notificación de cambio de elemento de configuración sobredimensionado a su bucket de Amazon S3. Verifique que ha especificado un bucket de Amazon S3 válido.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
```

```
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

Visualización del AWS Config panel

Usa el panel de control para ver un resumen de tus recursos, reglas, paquetes de conformidad y sus estados de conformidad, y para visualizar tus métricas de AWS Config uso y éxito con Amazon CloudWatch. Esta página le ayuda a identificar rápidamente los principales recursos de su AWS cuenta, los paquetes de conformidad con el nivel de cumplimiento más bajo Cuenta de AWS, qué reglas o recursos no cumplen con los requisitos en su cuenta Cuenta de AWS, qué tráfico impulsa su AWS Config uso y las métricas clave del éxito y el fracaso que se han producido en sus flujos de trabajo.

Para usar el panel AWS Config

1. Inicia sesión en la AWS Config consola de https://console.aws.amazon.com/config/tu casa Consola de administración de AWS y ábrela.
2. En el panel de navegación izquierdo, elija Panel.

Contenido

- Cumplimiento e inventario de recursos
- AWS Config Métricas de uso y éxito

Cumplimiento e inventario de recursos

Después de la configuración, AWS Config comienza a registrar los recursos especificados y a evaluarlos según sus reglas. Es posible que tarden unos minutos en AWS Config mostrarse los recursos, las reglas, los paquetes de conformidad y sus estados de conformidad.

Paquetes de conformidad por puntuación de conformidad

Los paquetes de conformidad por puntuación de conformidad muestran hasta 10 de los paquetes de conformidad con la puntuación de conformidad más baja. La puntuación de conformidad es el porcentaje del número de combinaciones de reglas y recursos conformes en un paquete de conformidad en comparación con el número total de combinaciones posibles de reglas y recursos en el paquete de conformidad.

Esta métrica le proporciona visión general del estado de cumplimiento de sus paquetes de conformidad y se puede utilizar para identificar, investigar y comprender el nivel de cumplimiento

de sus paquetes de conformidad. Puede utilizar la puntuación de conformidad para realizar un seguimiento del progreso de las soluciones, realizar comparaciones entre diferentes conjuntos de requisitos y ver el impacto que un cambio o implementación específicos tienen en un paquete de conformidad.

Para ver el estado de la implementación, la puntuación de cumplimiento, el plazo de la puntuación de cumplimiento y las reglas de un paquete de conformidad en una vista detallada, elija el nombre del paquete de conformidad en Paquete de conformidad.

Compliance status (Estado de conformidad)

El estado de conformidad muestra el número de normas y de recursos conformes y no conformes. Los recursos son conformes y no conformes en función de una evaluación de la regla asociada a ellos. Si un recurso no sigue las especificaciones de la regla, el recurso y la regla se marcan como no conformes.

Para ver la lista de reglas y recursos no conformes, seleccione Regla(s) no conforme(s) o Recurso(s) no conforme(s).

Reglas por recursos no conformes

Las reglas por recursos no conformes muestran las principales reglas no conformes en orden descendente según el número de recursos. Elija una regla para ver sus detalles, parámetros y los recursos incluidos en el ámbito de aplicación de esa regla específica.

Para obtener una lista completa de las reglas no conformes, seleccione Ver todas las reglas no conformes.

Inventario de recursos

El inventario de recursos muestra el número total de recursos que AWS Config se registra en orden descendente según el número de recursos y el recuento de cada tipo de recurso del suyo. Cuenta de AWS Para abrir todos los recursos de un tipo de recurso, elija ese tipo de recurso para ir a su página de inventario de recursos.

Puede usar la lista desplegable para indicar los totales de recursos que desea ver. De forma predeterminada, está configurado para ver todos los recursos, pero puedes cambiarlo a AWS Recursos, Recursos de terceros o Recursos personalizados.

> **Note**
>
> El mensaje Evalúe la configuración de sus AWS recursos mediante las reglas de Config puede aparecer en el panel de control por los siguientes motivos:
>
> - No has configurado AWS Config reglas para tu Cuenta de AWS. Puede elegir Add rule (Añadir regla) para ir a la página Rules (Reglas).
> - AWS Config sigue evaluando sus recursos en función de sus reglas. Puede actualizar la página para ver los últimos resultados de la evaluación.
> - AWS Config evaluó sus recursos en función de sus reglas y no encontró ningún recurso dentro del alcance. Puede especificar los recursos AWS Config que desea registrar en la página de configuración. Para obtener más información, consulte Grabación de AWS recursos con AWS Config.

AWS Config Métricas de uso y éxito

Puedes usar los CloudWatch paneles de Amazon en la AWS Config consola para visualizar tus métricas AWS Config de uso y éxito.

Para cada panel, puede hacer lo siguiente:

- Ajustar el intervalo de tiempo del panel para mostrar los datos desde hace 3 horas, 1 día o 1 semana.
- Seleccione el icono de calendario para introducir un rango de tiempo personalizado: un tiempo relativo para un período de tiempo específico pasado o un rango de tiempo absoluto entre dos fechas.
- Puede cambiar el formato de hora para que aparezcan los datos del panel en UTC (hora universal coordinada) o en la zona horaria local (la zona horaria especificada como local en el sistema operativo del dispositivo).
- Utilice la flecha desplegable junto al icono de actualización para especificar la frecuencia con la que deben actualizarse los datos de un panel o para desactivar la actualización automática. Elija Desactivada, 10 segundos, 1 minuto, 2 minutos, 5 minutos o 15 minutos para cambiar el intervalo de actualización.
- Selecciona Más opciones (el menú de puntos suspensivos verticales) para añadir a la consola las métricas de AWS Config uso o de AWS Config éxito que estás viendo actualmente en el AWS Config panel de control. CloudWatch Esto abre una nueva pestaña en la CloudWatch consola

que te permite crear un nuevo panel personalizado CloudWatch con información copiada de tus métricas de AWS Config uso o de AWS Config éxito actuales.

Si desea realizar análisis adicionales de estas métricas con CloudWatch, elija Métricas en el panel de navegación izquierdo de la CloudWatch consola y, a continuación, elija AWS/Config. Para obtener más información sobre lo que puede hacer desde la CloudWatch consola, consulte Uso de CloudWatch paneles de Amazon y Uso de CloudWatch métricas de Amazon en la Guía del CloudWatch usuario.

AWS Config Métricas de uso

Métrica	Description (Descripción)	Unidad	
`Configuration Items Recorded`	El número de elementos de configuración registrados para cada tipo de recurso o para todos los tipos de recurso. Un elemento de configuración representa una point-in-time vista de los diversos atributos de un AWS recurso compatible. Para obtener más información sobre los elementos de configuración o los tipos de recursos compatibles, consulte Elementos de configuración y Tipos de recursos compatibles.	Recuento	

Puede seleccionar el tipo de recurso que desea ver mediante la lista desplegable. De forma predeterminada, está configurada para mostrar todos los tipos de recurso.

AWS Config Métricas de éxito

Métrica	Description (Descripción)	Unidad	
`Change Notifications Delivery Failed`	El número de envíos fallidos de notificaciones de cambio al tema de Amazon SNS correspondiente al canal de entrega. Una notificación de cambio le informa sobre un cambio en el estado de la configuración de sus AWS recursos. Puede usar la	Recuento	

Métrica	Description (Descripción)	Unidad	
	ConfigStreamDeliveryInfoAPI para obtener la notificación de cambio `lastErrorCode` o `lastErrorMessage` para el último intento de entrega de una notificación de cambio. Para obtener más información, consulte Administrar el canal de entrega.		
`Config History Export Failed`	El número de exportaciones fallidas del historial de configuración al bucket de Amazon S3. Un historial de configuración es una colección de elementos de configura ción de un recurso determinado durante un periodo de tiempo específico. Para obtener más información sobre el historial de configuración, consulte Historial de configura ción.	Recuento	
`Configura tion Recorder Insuffici ent Permissio ns Failure`	El número de intentos fallidos de acceso a los permisos debidos a la política de funciones de IAM para todos los grabadore s de configuración de tu cuenta y a Región de AWS que los permisos son insuficie ntes. El registrador de configuración detecta los cambios en los tipos de recursos del ámbito. Para que el grabador de configura ción registre las configuraciones AWS de los recursos, necesita los permisos de IAM necesarios. Para obtener más información, consulte la Política de roles de IAM para obtener datos de configuración.	Recuento	

Métrica	Description (Descripción)	Unidad	
`Config Snapshot Export Failed`	El número de exportaciones fallidas de instantáneas de configuración al bucket de Amazon S3. Una instantánea de configura ción es una colección de elementos de configuración para los recursos admitidos en su cuenta. Para obtener más informaci ón sobre las instantáneas de configuración, consulte Instantánea de configuración.	Recuento	

Administración y visualización de configuraciones AWS de recursos con AWS Config

AWS Config permite evaluar, auditar y evaluar las configuraciones de AWS los recursos.

AWS los recursos son entidades que se crean y administran mediante las Consola de administración de AWS herramientas AWS Command Line Interface (CLI) o AWS asociadas. AWS SDKs Entre los ejemplos de AWS recursos se incluyen las instancias de Amazon EC2, los grupos de seguridad VPCs, Amazon y Amazon Elastic Block Store. AWS Config hace referencia a cada recurso mediante su identificador único, como el ID del recurso o un nombre de recurso de Amazon (ARN).

Estos son algunos casos de uso comunes:

- Administrador de la nube: puede realizar un seguimiento de las configuraciones de los recursos y administrarlas para garantizar el cumplimiento, solucionar problemas y mantener una comprensión de su entorno AWS
- Analista de seguridad: puede evaluar las configuraciones de los recursos comparándolas con los estados deseados a fin de identificar las vulnerabilidades y evaluar la postura de seguridad.
- Responsable de cumplimiento: puede auditar y supervisar de forma continua las configuraciones de los recursos para garantizar el cumplimiento de las políticas organizativas y las normativas del sector.

Temas

- Tipos de recursos compatibles para AWS Config
- Cobertura de los recursos según la disponibilidad por región
- Grabación de AWS recursos con AWS Config
- Grabación de configuraciones con AWS Config recursos de terceros mediante AWS CLI
- Configuración del software de grabación para instancias administradas con AWS Config
- Búsqueda de recursos descubiertos por AWS Config
- Visualización de la información de cumplimiento y los resultados de la evaluación de sus AWS recursos con AWS Config
- Ver el historial de cumplimiento de sus AWS recursos con AWS Config
- Consulta el historial de conformidad de sus recursos AWS
- Etiquetado de los recursos de AWS Config

Tipos de recursos compatibles para AWS Config

> **Important**
>
> Esta página se actualiza mensualmente, al principio de cada mes.

AWS Config admite los siguientes tipos de AWS recursos y relaciones de recursos.

- Para obtener información más detallada sobre un tipo de recurso, consulte su información de referencia (como la sintaxis, las propiedades y los valores devueltos) en la referencia sobre los tipos de AWS recursos y propiedades de la Guía del AWS CloudFormation usuario.
- Para el AWS Config registro, algunas AWS regiones admiten un subconjunto de estos tipos de recursos. Para obtener información sobre los tipos de recursos admitidos en determinadas regiones, consulte Cobertura de recursos según la disponibilidad por región.
- Las consultas avanzadas AWS Config admiten un subconjunto de estos tipos de recursos. Para ver una lista de tipos de recursos compatibles, consulte Tipos de recursos compatibles para consultas avanzadas.
- La evaluación proactiva AWS Config admite un subconjunto de estos tipos de recursos. Para obtener una lista de esos tipos de recursos compatibles, consulte Tipos de recursos compatibles para la evaluación proactiva.
- Las reglas periódicas se ejecutan sin que el registrador de configuración esté habilitado, ya que las reglas periódicas no dependen de los elementos de configuración (CIs). Para obtener más información sobre la diferencia entre las reglas activadas por cambios y las reglas periódicas, consulte Modo de evaluación y Tipos de activación de las AWS Config reglas.

  Esto significa que si ve la página de reglas, no aparece ningún CI ni recurso compatible en la lista. Si selecciona el ID del recurso, aparecerá el siguiente error: `The provided resource ID and resource type cannot be found`. Este es el comportamiento esperado.

> **Note**
>
> Disponibilidad regional para tipos de recursos
> Antes de especificar un tipo de recurso AWS Config para el seguimiento, compruebe la cobertura de los recursos por región y la disponibilidad para comprobar si el tipo de recurso es compatible con la AWS región en la que lo configuró. AWS Config Si al menos una región

admite un tipo de recurso, puede habilitar el registro de ese tipo de recurso en todas las regiones admitidas AWS Config, incluso si el tipo de recurso especificado no es compatible con la AWS región en la que lo configuró AWS Config. AWS Config

Compatibilidad con el etiquetado para tipos de recursos

Si un tipo de recurso no admite el etiquetado o no incluye información sobre las etiquetas en su respuesta a la API descrita, AWS Config no capturará los datos de las etiquetas en los elementos de configuración (CIs) de ese tipo de recurso. AWS Config seguirá registrando estos recursos. Sin embargo, cualquier funcionalidad que dependa de los datos de las etiquetas no funcionará. Esto afecta al filtrado, la agrupación o la evaluación del cumplimiento que se basan en los datos de las etiquetas.

Amazon AppStream

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon AppStream	`AWS::AppStream::Application`	N/A	N/A
	`AWS::AppStream::AppBlockBuilder`	N/A	N/A
	`AWS::AppStream::DirectoryConfig`	N/A	N/A
	`AWS::AppStream::Fleet`	N/A	N/A
	`AWS::AppStream::Stack`	N/A	N/A

Amazon AppFlow

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon AppFlow	`AWS::AppFlow::Flow`	N/A	N/A

Amazon AppIntegrations

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon AppIntegrations	`AWS::AppIntegrations::EventIntegration`	N/A	N/A
	`AWS::AppIntegrations::Application`	N/A	N/A

Amazon API Gateway

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
API Gateway	`AWS::ApiGateway::DomainName`	N/A	N/A
	`AWS::ApiGateway::Stage`	está incluido en	ApiGateway API de descanso

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
		está asociado a	WAFRegional WebACL
	`AWS::ApiGateway::Method`	N/D	Etapa NA
	`AWS::ApiGateway::RestApi`	contains	ApiGateway Escenario
	`AWS::ApiGateway::UsagePlan`	N/A	N/A
API Gateway V2	`AWS::ApiGatewayV2::Stage`	está incluido en	ApiGatewayV2 Api
	`AWS::ApiGatewayV2::Api`	contains	ApiGatewayEtapa V2
	`AWS::ApiGatewayV2::Integration`	N/A	N/A

Para obtener más información sobre cómo AWS Config se integra con Amazon API Gateway, consulte Supervisión de la configuración de API de API Gateway con AWS Config.

Amazon Athena

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Athena	`AWS::Athena::WorkGroup`	N/A	N/A
	`AWS::Athena::DataCatalog`	N/A	N/A
	`AWS::Athena::PreparedStatement`	N/A	N/A

Amazon Bedrock

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Bedrock	`AWS::Bedrock::ApplicationInferenceProfile`	N/A	N/A
	`AWS::Bedrock::Guardrail`	N/A	N/A
	`AWS::Bedrock::KnowledgeBase`	N/A	N/A
	`AWS::Bedrock::Prompt`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::BedrockAgentCore::BrowserCustom`	N/A	N/A
	`AWS::BedrockAgentCore::CodeInterpreterCustom`	N/A	N/A
	`AWS::BedrockAgentCore::Runtime`	N/A	N/A

Amazon CloudFront

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon CloudFront	`AWS::CloudFront::Distribution`	está asociado a	AWS WebACL WAF
			Certificado del ACM
			Bucket de S3
			Certificado de servidor de IAM
	`AWS::CloudFront::KeyValueStore`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::CloudFront::PublicKey`	N/A	N/A
	`AWS::CloudFront::StreamingDistribution`	está asociado a	AWS WebACL WAF
			Certificado del ACM
			Bucket de S3
			Certificado de servidor de IAM
	`AWS::CloudFront::RealtimeLogConfig`	N/A	N/A

Amazon CloudWatch

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	N/A	N/A
	`AWS::CloudWatch::MetricStream`	N/A	N/A
Amazon CloudWatch Logs	`AWS::Logs::Destination`	N/A	N/A
Amazon CloudWatch RUM	`AWS::RUM::AppMonitor`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon, CloudWatch evidentemente	`AWS::Evidently::Project`	N/A	N/A
	`AWS::Evidently::Launch`	N/A	N/A
	`AWS::Evidently::Segment`	N/A	N/A

Amazon CodeGuru

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
CodeGuru Revisor de Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	N/A	N/A
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	N/A	N/A

Amazon Cognito

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Cognito	`AWS::Cognito::UserPool`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::Cognito::UserPoolClient`	N/A	N/A
	`AWS::Cognito::UserPoolGroup`	N/A	N/A
	`AWS::Cognito::IdentityPool`	N/A	N/A

Amazon Comprehend

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Comprehend	`AWS::Comprehend::Flywheel`	N/A	N/A

Amazon Connect

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Connect	`AWS::Connect::PhoneNumber`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::Connect::QuickConnect`	N/A	N/A
	`AWS::Connect::Instance`	N/A	N/A
	`AWS::Connect::Rule`	N/A	N/A
	`AWS::Connect::SecurityProfile`	N/A	N/A
	`AWS::Connect::User`	N/A	N/A
Perfiles de clientes de Amazon Connect	`AWS::CustomerProfiles::Domain`	N/A	N/A
	`AWS::CustomerProfiles::ObjectType`	N/A	N/A

Amazon Detective

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Detective	`AWS::Detective::Graph`	N/A	N/A

Amazon DynamoDB

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon DynamoDB	`AWS::DynamoDB::Table`	N/A	N/A

Amazon Elastic Compute Cloud

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Elastic Compute Cloud	`AWS::EC2::Host` *	contains	Instancia de EC2
	`AWS::EC2::EIP`	está conectado a	Instancia de EC2
			Interfaz de red
	`AWS::EC2::Instance`	contains	Interfaz de red de EC2
		está asociado a	Grupo de seguridad de EC2
		está conectado a	Volumen de Amazon EBS
			IP elástica de EC2 (EIP)
		está incluido en	Host dedicado de EC2
			Tabla de enrutamiento
			Subred

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
			Nube privada virtual (VPC)
	`AWS::EC2::NetworkInterface`	está asociado a	Grupo de seguridad de EC2
		está conectado a	IP elástica de EC2 (EIP)
			Instancia de EC2
		está incluido en	Tabla de enrutamiento
			Subred
			Nube privada virtual (VPC)
	`AWS::EC2::SecurityGroup` *	está asociado a	Instancia de EC2
			Interfaz de red de EC2
			Nube privada virtual (VPC)
	`AWS::EC2::NatGateway`	está incluido en	Nube virtual privada (VPC)
		está incluido en	Subred
	`AWS::EC2::EgressOnlyInternetGateway`	está conectado a	Nube privada virtual (VPC)

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::EC2::EC2Fleet`	N/A	N/A
	`AWS::EC2::SpotFleet`	N/A	N/A
	`AWS::EC2::SubnetNetworkAclAssociation`	N/A	N/A
	`AWS::EC2::PrefixList`	N/A	N/A
	`AWS::EC2::FlowLog`	N/A	N/A
	`AWS::EC2::TransitGateway`	N/A	N/A
	`AWS::EC2::TransitGatewayAttachment`	N/A	N/A
	`AWS::EC2::TransitGatewayRouteTable`	N/A	N/A
	`AWS::EC2::VPCEndpoint`	está incluido en	Virtual Private Cloud (VPC)
		está conectado a	Interfaz de red

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
		está incluido en	Subred
		está incluido en	Tabla de enrutamiento
	`AWS::EC2::VPCEndpointService`	está asociado a	ElasticLoadBalancingV2 LoadBalancer
	`AWS::EC2::VPCPeeringConnection`	está asociado a	Nube privada virtual (VPC)
	`AWS::EC2::RegisteredHAInstance`	está asociado a	Instancia de EC2
	`AWS::EC2::SubnetRouteTableAssociation`	N/A	N/A
	`AWS::EC2::LaunchTemplate`	N/A	N/A
	`AWS::EC2::NetworkInsightsAccessScopeAnalysis`	N/A	N/A
	`AWS::EC2::TrafficMirrorTarget`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::EC2::TrafficMirrorSession`	N/A	N/A
	`AWS::EC2::DHCPOptions`	N/A	N/A
	`AWS::EC2::IPAM`	N/A	N/A
	`AWS::EC2::IPAMResourceDiscovery`	N/A	N/A
	`AWS::EC2::IPAMResourceDiscoveryAssociation`	N/A	N/A
	`AWS::EC2::NetworkInsightsPath`	N/A	N/A
	`AWS::EC2::TrafficMirrorFilter`	N/A	N/A
	`AWS::EC2::CapacityReservation`	N/A	N/A
	`AWS::EC2::ClientVpnEndpoint`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::EC2::Customer Gateway`	está conectado a	Conexión de VPN
	`AWS::EC2::Internet Gateway`	está conectado a	Nube privada virtual (VPC)
	`AWS::EC2::NetworkAcl`	N/A	N/A
	`AWS::EC2::RouteTable`	contains	Instancia de EC2
			Interfaz de red de EC2
			Subred
			Puerta de enlace de VPN
		está incluido en	Nube privada virtual (VPC)
	`AWS::EC2::Subnet`	contains	Instancia de EC2
			Interfaz de red de EC2
		está conectado a	ACL de red
		está incluido en	Tabla de enrutamie nto
			Nube privada virtual (VPC)

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::EC2::VPC`	contains	Instancia de EC2
			Interfaz de red de EC2
			ACL de red
			Tabla de enrutamiento
			Subred
		está asociado a	Grupo de seguridad
		está conectado a	Puerta de enlace de Internet
			Puerta de enlace de VPN
	`AWS::EC2::VPNConnection`	está conectado a	Puerta de enlace de cliente
			Puerta de enlace de VPN
	`AWS::EC2::VPNConnectionRoute`	N/A	N/A
	`AWS::EC2::VPNGateway`	está conectado a	Nube privada virtual (VPC)
			Conexión de VPN
		está incluido en	Tabla de enrutamiento

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::EC2::IPAMScope`	N/A	N/A
	`AWS::EC2::CarrierGateway`	N/A	N/A
	`AWS::EC2::TransitGatewayConnect`	N/A	N/A
	`AWS::EC2::IPAMPool`	N/A	N/A
	`AWS::EC2::TransitGatewayMulticastDomain`	N/A	N/A
	`AWS::EC2::NetworkInsightsAccessScope`	N/A	N/A
	`AWS::EC2::NetworkInsightsAnalysis`	N/A	N/A
	`AWS::EC2::VPCBlockPublicAccessOptions`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::EC2::VPCBlockPublicAccessExclusion`	N/A	N/A
	`AWS::EC2::EIPAssociation`	N/A	N/A
	`AWS::EC2::InstanceConnectEndpoint`	N/A	N/A
	`AWS::EC2::SnapshotBlockPublicAccess`	N/A	N/A
	`AWS::EC2::VPCEndpointConnectionNotification`	N/A	N/A
	`AWS::EC2::SecurityGroupVpcAssociation`	N/A	N/A
	`AWS::EC2::VerifiedAccessInstance`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::EC2::IPAMPoolCidr`	N/A	N/A
	`AWS::EC2::SubnetCidrBlock`	N/A	N/A
	`AWS::EC2::VPCGatewayAttachment`	N/A	N/A
Amazon Elastic Block Store	`AWS::EC2::Volume`	está conectado a	Instancia de EC2
Generador de Imágenes de EC2	`AWS::ImageBuilder::ContainerRecipe`	N/A	N/A
	`AWS::ImageBuilder::DistributionConfiguration`	N/A	N/A
	`AWS::ImageBuilder::ImagePipeline`	N/A	N/A
	`AWS::ImageBuilder::ImageRecipe`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::ImageBuilder::InfrastructureConfiguration`	N/A	N/A
	`AWS::ImageBuilder::LifecyclePolicy`	N/A	N/A

*AWS Config registra los detalles de configuración de los hosts dedicados y las instancias que se lanzan en ellos. Como resultado, puede utilizarlos AWS Config como fuente de datos al informar sobre el cumplimiento de sus licencias de software vinculadas a servidores. Por ejemplo, puede ver el historial de configuración de una instancia y determinar en qué imagen de máquina de Amazon (AMI) se basa. A continuación, puede consultar el historial de configuración del host, que incluye información como el número de sockets y núcleos, para comprobar que el host cumple los requisitos de licencia de la AMI. Para obtener más información, consulte Realice el seguimiento de los cambios mediante AWS Config en la Guía del usuario de Amazon EC2.

* La definición de SecurityGroup propiedades de EC2 contiene bloques CIDR de IP, que se convierten internamente en rangos de IP y pueden arrojar resultados inesperados al intentar encontrar un rango de IP específico. Para obtener soluciones alternativas para buscar rangos de IP específicos, consulte Limitaciones de las consultas avanzadas.

Amazon Elastic Container Registry

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Elastic Container Registry	`AWS::ECR::Replicat`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`ionConfiguration`		
	`AWS::ECR::Repository`	N/A	N/A
	`AWS::ECR::RepositoryCreationTemplate`	N/A	N/A
	`AWS::ECR::RegistryPolicy`	N/A	N/A
	`AWS::ECR::PullThroughCacheRule`	N/A	N/A
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	N/A	N/A

Amazon Elastic Container Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Elastic Container Service	`AWS::ECS::Cluster`	N/A	N/A
	`AWS::ECS::TaskDefinition`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::ECS::Service` *	N/A	N/A
	`AWS::ECS::TaskSet`	N/A	N/A
	`AWS::ECS::Capacity Provider`	N/A	N/A

*En la actualidad, este servicio solo admite el nuevo formato de nombre de recurso de Amazon (ARN). Para obtener más información, consulte Amazon Resource Names (ARNs) y IDs en la guía para desarrolladores de ECS.

Antiguo (no compatible): `arn:aws:ecs:`*`region`*`:`*`aws_account_id`*`:service/`*`service-name`*

Nuevo (compatible): `arn:aws:ecs:`*`region`*`:`*`aws_account_id`*`:service/`*`cluster-name`*`/`*`service-name`*

Amazon Elastic File System

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Elastic File System	`AWS::EFS::FileSystem`	N/A	N/A
	`AWS::EFS::AccessPoint`	N/A	N/A

Amazon Elastic Kubernetes Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Elastic Kubernetes Service	`AWS::EKS::Cluster`	N/A	N/A
	`AWS::EKS::FargateProfile`	N/A	N/A
	`AWS::EKS::IdentityProviderConfig`	N/A	N/A
	`AWS::EKS::Addon`	N/A	N/A

Amazon EMR

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon EMR	`AWS::EMR::Studio`	N/A	N/A
	`AWS::EMR::SecurityConfiguration`	N/A	N/A
Contenedores de Amazon EMR	`AWS::EMRContainers::VirtualCluster`	N/A	N/A

Amazon EMR sin servidor

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon EMR sin servidor	`AWS::EMRServerless::Application`	N/A	N/A

Amazon EventBridge

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon EventBridge	`AWS::Events::EventBus`	N/A	N/A
	`AWS::Events::ApiDestination`	N/A	N/A
	`AWS::Events::Archive`	N/A	N/A
	`AWS::Events::Endpoint`	N/A	N/A
	`AWS::Events::Connection`	N/A	N/A
	`AWS::Events::Rule`	N/A	N/A
EventBridge Esquemas de Amazon	`AWS::EventSchemas::RegistryPolicy`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::EventSchemas::Discoverer`	N/A	N/A
	`AWS::EventSchemas::Schema`	N/A	N/A
	`AWS::EventSchemas::Registry`	N/A	N/A

Amazon Forecast

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Forecast	`AWS::Forecast::Dataset`	N/A	N/A
	`AWS::Forecast::DatasetGroup`	N/A	N/A

Amazon Fraud Detector

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Fraud Detector	`AWS::FraudDetector::Label`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::FraudDetector::EntityType`	N/A	N/A
	`AWS::FraudDetector::Variable`	N/A	N/A
	`AWS::FraudDetector::Outcome`	N/A	N/A

Amazon GameLift

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon GameLift	`AWS::GameLift::Build`	N/A	N/A

Amazon GuardDuty

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon GuardDuty	`AWS::GuardDuty::Detector`	N/A	N/A
	`AWS::GuardDuty::Filter`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::GuardDuty::IPSet`	N/A	N/A
	`AWS::GuardDuty::MalwareProtectionPlan`	N/A	N/A
	`AWS::GuardDuty::ThreatIntelSet`	N/A	N/A

Amazon Inspector

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Inspector	`AWS::InspectorV2::Filter`	N/A	N/A
	`AWS::InspectorV2::Activation`	N/A	N/A

Amazon Interactive Video Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Interactive Video Service	`AWS::IVS::Channel`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::IVS::RecordingConfiguration`	N/A	N/A
	`AWS::IVS::PlaybackKeyPair`	N/A	N/A

Amazon Keyspaces (para Apache Cassandra)

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Keyspaces (para Apache Cassandra)	`AWS::Cassandra::Keyspace`	N/A	N/A

Amazon Location Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Location Service	`AWS::Location::APIKey`	N/A	N/A

OpenSearch Servicio Amazon

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon OpenSearch Service (versión antigua de Elasticsearch)	`AWS::Elasticsearch::Domain`	está asociado a	Clave de KMS
			Grupo de seguridad de EC2
			Subred EC2
			Nube privada virtual (VPC)
OpenSearch Servicio Amazon	`AWS::OpenSearch::Domain`	N/A	N/A
Amazon OpenSearch Serverless	`AWS::OpenSearchServerless::VpcEndpoint`	N/A	N/A
	`AWS::OpenSearchServerless::Collection`	N/A	N/A
	`AWS::OpenSearchServerless::SecurityConfig`	N/A	N/A

> **Cambio de nombre OpenSearch de Amazon Service**
>
> El 8 de septiembre de 2021, Amazon Elasticsearch Service pasó a llamarse Amazon Service. OpenSearch OpenSearch El servicio también es compatible con OpenSearch el

sistema operativo Elasticsearch heredado. Para obtener más información, consulta Amazon OpenSearch Service: resumen de cambios.
Es posible que sigas viendo tus datos `AWS::OpenSearch::Domain` en el tipo de `AWS::Elasticsearch::Domain` recurso existente durante varias semanas, incluso si actualizas uno o más dominios a ellos OpenSearch.

Amazon Personalize

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Personalize	`AWS::Personalize::Dataset`	N/A	N/A
	`AWS::Personalize::Schema`	N/A	N/A
	`AWS::Personalize::Solution`	N/A	N/A
	`AWS::Personalize::DatasetGroup`	N/A	N/A

Amazon Pinpoint

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Pinpoint	`AWS::Pinpoint::App`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`licationSettings`		
	`AWS::Pinpoint::Segment`	N/A	N/A
	`AWS::Pinpoint::App`	N/A	N/A
	`AWS::Pinpoint::Campaign`	N/A	N/A
	`AWS::Pinpoint::InAppTemplate`	N/A	N/A
	`AWS::Pinpoint::EmailChannel`	N/A	N/A
	`AWS::Pinpoint::EmailTemplate`	N/A	N/A
	`AWS::Pinpoint::EventStream`	N/A	N/A

Amazon Quantum Ledger Database (Amazon QLDB)

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon QLDB	`AWS::QLDB::Ledger`	N/A	N/A

Amazon Kendra

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Kendra	`AWS::Kendra::Index`	N/A	N/A

Amazon Kinesis

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Kinesis	`AWS::Kinesis::Stream`	N/A	N/A
	`AWS::Kinesis::StreamConsumer`	N/A	N/A
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	N/A	N/A
Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`	N/A	N/A
Kinesis Video Streams	`AWS::KinesisVideo::SignalingChannel`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::KinesisVideo::Stream`	N/A	N/A

Amazon Lex

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Lex	`AWS::Lex::BotAlias`	N/A	N/A
	`AWS::Lex::Bot`	N/A	N/A

Amazon Lightsail

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Lightsail	`AWS::Lightsail::Disk`	N/A	N/A
	`AWS::Lightsail::Certificate`	N/A	N/A
	`AWS::Lightsail::Bucket`	N/A	N/A
	`AWS::Lightsail::StaticIp`	N/A	N/A

Amazon Lookout for Metrics

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Lookout for Metrics	`AWS::LookoutMetrics::Alert`	N/A	N/A

Amazon Lookout for Vision

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Lookout for Vision	`AWS::LookoutVision::Project`	N/A	N/A

Amazon Macie

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Macie	`AWS::Macie::Session`	N/A	N/A

Amazon Managed Grafana

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Managed Grafana	`AWS::Grafana::Workspace`	N/A	N/A

Servicio administrado por Amazon para Prometheus

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Servicio administrado por Amazon para Prometheus	`AWS::APS::RuleGroupsNamespace`	N/A	N/A

Amazon MemoryDB

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon MemoryDB	`AWS::MemoryDB::SubnetGroup`	N/A	N/A

Amazon MQ

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon MQ	`AWS::AmazonMQ::Broker`	N/A	N/A

Transmisión administrada de Amazon para Apache Kafka

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Transmisión administrada de Amazon para Apache Kafka	`AWS::MSK::Cluster`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::MSK::Configuration`	N/A	N/A
	`AWS::MSK::BatchScramSecret`	N/A	N/A
	`AWS::MSK::ClusterPolicy`	N/A	N/A
	`AWS::MSK::ServerlessCluster`	N/A	N/A
	`AWS::MSK::VpcConnection`	N/A	N/A
Amazon Managed Streaming para Apache Kafka Connect	`AWS::KafkaConnect::Connector`	N/A	N/A
	`AWS::KafkaConnect::CustomPlugin`	N/A	N/A

Amazon Quick

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Quick	`AWS::QuickSight::DataSource`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::QuickSight::Template`	N/A	N/A
	`AWS::QuickSight::Theme`	N/A	N/A

Amazon Redshift

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Redshift	`AWS::Redshift::Cluster`	está asociado a	Grupo de parámetros del clúster
			Grupo de seguridad de clúster
			Grupo de subredes de clúster
			Security group (Grupo de seguridad)
			Nube privada virtual (VPC)
	`AWS::Redshift::ClusterParameterGroup`	N/A	N/A
	`AWS::Redshift::Clu`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`sterSecurityGroup`		
	`AWS::Redshift::ScheduledAction`	N/A	N/A
	`AWS::Redshift::ClusterSnapshot`	está asociado a	Clúster
			Nube privada virtual (VPC)
	`AWS::Redshift::ClusterSubnetGroup`	está asociado a	Subred
			Nube privada virtual (VPC)
	`AWS::Redshift::EventSubscription`	N/A	N/A
	`AWS::Redshift::EndpointAccess`	N/A	N/A
	`AWS::Redshift::EndpointAuthorization`	N/A	N/A
	`AWS::Redshift::Integration`	N/A	N/A

Amazon Relational Database Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Relational Database Service	`AWS::RDS::DBCluster`	contains	Instancia de base de datos de RDS
		está asociado a	Grupo de subred de base de datos de RDS
			Grupo de seguridad de EC2
	`AWS::RDS::DBClusterSnapshot`	está asociado a	Clúster de base de datos de RDS
			Nube privada virtual (VPC)
	`AWS::RDS::DBInstance`	está asociado a	Grupo de seguridad de EC2
			Grupo de seguridad de base de datos de RDS
			Grupo de subred de base de datos de RDS
	`AWS::RDS::DBSecurityGroup`	está asociado a	Grupo de seguridad de EC2
			Nube privada virtual (VPC)

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::RDS::DBSnapshot`	está asociado a	Nube privada virtual (VPC)
	`AWS::RDS::DBSubnetGroup`	está asociado a	Grupo de seguridad de EC2
			Nube privada virtual (VPC)
	`AWS::RDS::EventSubscription`	N/A	N/A
	`AWS::RDS::GlobalCluster`	N/A	N/A
	`AWS::RDS::Integration`	N/A	N/A
	`AWS::RDS::OptionGroup`	N/A	N/A

Amazon Route 53

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Route 53	`AWS::Route53::DNSSEC`	N/A	N/A
	`AWS::Route53::HostedZone`	N/A	N/A
	`AWS::Route53::HealthCheck`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Perfiles de Amazon Route 53	`AWS::Route53Profiles::Profile`	N/A	N/A
	`AWS::Route53Profiles::ProfileAssociation`	N/A	N/A
Amazon Route 53 Resolver	`AWS::Route53Resolver::ResolverEndpoint`	N/A	N/A
	`AWS::Route53Resolver::ResolverRule`	N/A	N/A
	`AWS::Route53Resolver::ResolverRuleAssociation`	N/A	N/A
	`AWS::Route53Resolver::FirewallDomainList`	N/A	N/A
	`AWS::Route53Resolver::FirewallRuleGroupAssociation`	N/A	N/A
	`AWS::Route53Resolver::ResolverQueryLoggingConfig`	N/A	N/A
	`AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation`	N/A	N/A
	`AWS::Route53Resolver::FirewallRuleGroup`	N/A	N/A
Controlador de recuperación de aplicaciones (ARC) de Amazon	`AWS::Route53RecoveryReadiness::Cell`	N/A	N/A
	`AWS::Route53RecoveryReadiness::ReadinessCheck`	N/A	N/A
	`AWS::Route53RecoveryReadiness::RecoveryGroup`	N/A	N/A
	`AWS::Route53RecoveryControl::Cluster`	N/A	N/A
	`AWS::Route53RecoveryControl::ControlPanel`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::Route53RecoveryControl::RoutingControl`	N/A	N/A
	`AWS::Route53RecoveryControl::SafetyRule`	N/A	N/A
	`AWS::Route53RecoveryReadiness::ResourceSet`	N/A	N/A

Amazon SageMaker AI

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon SageMaker AI	`AWS::SageMaker::AppImageConfig`	N/A	N/A
	`AWS::SageMaker::CodeRepository`	N/A	N/A
	`AWS::SageMaker::DataQualityJobDefinition`	N/A	N/A
	`AWS::SageMaker::Domain`	N/A	N/A
	`AWS::SageMaker::En`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado	
	dpointConfig			
	AWS::SageMaker::FeatureGroup	N/A	N/A	
	AWS::SageMaker::Image	N/A	N/A	
	AWS::SageMaker::InferenceExperiment	N/A	N/A	
	AWS::SageMaker::MlflowTrackingServer	N/A	N/A	
	AWS::SageMaker::Model	N/A	N/A	
	AWS::SageMaker::ModelBiasJobDefinition	N/A	N/A	

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado	
	`AWS::SageMaker::ModelExplainabilityJobDefinition`	N/A	N/A	
	`AWS::SageMaker::ModelQualityJobDefinition`	N/A	N/A	
	`AWS::SageMaker::MonitoringSchedule`	N/A	N/A	
	`AWS::SageMaker::NotebookInstance`	N/A	N/A	
	`AWS::SageMaker::NotebookInstanceLifecycleConfig`	N/A	N/A	
	`AWS::SageMaker::StudioLifecycleConfig`	N/A	N/A	

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado	
	`AWS::SageMaker::UserProfile`	N/A	N/A	
`AWS::SageMaker::Workteam`	N/A	N/A		

Amazon Simple Email Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Simple Email Service	`AWS::SES::ConfigurationSet`	N/A	N/A
	`AWS::SES::ContactList`	N/A	N/A
	`AWS::SES::DedicatedIpPool`	N/A	N/A
	`AWS::SES::MailManagerTrafficPolicy`	N/A	N/A
	`AWS::SES::Template`	N/A	N/A
	`AWS::SES::ReceiptFilter`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::SES::ReceiptRuleSet`	N/A	N/A

Amazon Simple Notification Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Simple Notification Service	`AWS::SNS::Topic`	N/A	N/A

Amazon Simple Queue Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Simple Queue Service	`AWS::SQS::Queue`	N/A	N/A

Amazon Simple Storage Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon Simple Storage Service	`AWS::S3::Bucket` *	N/A	N/A
	`AWS::S3::AccountPu`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`blicAccessBlock`		
	`AWS::S3::MultiRegionAccessPoint`	N/A	N/A
	`AWS::S3::StorageLens`	N/A	N/A
	`AWS::S3::AccessGrant`	N/A	N/A
	`AWS::S3::AccessGrantsInstance`	N/A	N/A
	`AWS::S3::AccessGrantsLocation`	N/A	N/A
	`AWS::S3::AccessPoint`	N/A	N/A
	`AWS::S3::StorageLensGroup`	N/A	N/A
	`AWS::S3Tables::TableBucket`	N/A	N/A
	`AWS::S3Tables::TableBucketPolicy`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon S3 Express One Zone	`AWS::S3Express::DirectoryBucket`	N/A	N/A
	`AWS::S3Express::BucketPolicy`	N/A	N/A

* Si lo configuró AWS Config para registrar sus buckets de S3 y no recibe notificaciones de cambios de configuración, compruebe que las políticas de sus buckets de S3 tengan los permisos necesarios. Para obtener más información, consulte Administración de permisos para el registro de buckets de S3.

Atributos del bucket de Amazon S3

AWS Config también registra los siguientes atributos para el tipo de recurso de bucket de Amazon S3.

Atributos	Description (Descripción)
AccelerateConfiguration	Transfer Acceleration de datos a largas distancias entre su cliente y un bucket.
BucketAcl	Lista de control de acceso que se utiliza para administrar el acceso a buckets y objetos.
BucketPolicy	Política que define los permisos para acceder al bucket.
CrossOriginConfiguration	Permitir solicitudes entre orígenes al bucket.
LifecycleConfiguration	Normas que definen el ciclo de vida de los objetos en el bucket.
LoggingConfiguration	Registro que se utiliza para realizar un seguimiento de las solicitudes de acceso al bucket.

Atributos	Description (Descripción)
NotificationConfiguration	Las notificaciones de eventos que se utilizan para enviar alertas o activar flujos de trabajo para eventos especificados de bucket.
ReplicationConfiguration	Copia asincrónica y automática de los objetos en buckets de diferentes regiones de AWS .
RequestPaymentConfiguration	Se ha habilitado el pago por solicitante.
TaggingConfiguration	Se han añadido etiquetas al bucket para categorizar. También puede utilizar el etiquetado para realizar un seguimiento de la facturación.
WebsiteConfiguration	Se ha habilitado el alojamiento de sitios web estáticos para el bucket.
VersioningConfiguration	Se ha habitado el control de versiones para objetos en el bucket.

Para obtener más información acerca de los atributos, consulte Opciones de configuración de buckets en la Guía del usuario de Amazon Simple Storage Service.

Amazon WorkSpaces

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Amazon WorkSpaces	`AWS::WorkSpaces::ConnectionAlias`	N/A	N/A
	`AWS::WorkSpaces::Workspace`	N/A	N/A

AWS Amplify

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Amplify	`AWS::Amplify::App`	N/A	N/A
	`AWS::Amplify::Branch`	N/A	N/A

AWS AppConfig

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS AppConfig	`AWS::AppConfig::Application`	N/A	N/A
	`AWS::AppConfig::Environment`	N/A	N/A
	`AWS::AppConfig::ConfigurationProfile`	N/A	N/A
	`AWS::AppConfig::DeploymentStrategy`	N/A	N/A
	`AWS::AppConfig::HostedConfi`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`gurationVersion`		
	`AWS::AppConfig::Extension`	N/A	N/A
	`AWS::AppConfig::ExtensionAssociation`	N/A	N/A

AWS App Runner

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS App Runner	`AWS::AppRunner::VpcConnector`	N/A	N/A
	`AWS::AppRunner::Service`	N/A	N/A

AWS App Mesh

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS App Mesh	`AWS::AppMesh::VirtualNode`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::AppMesh::VirtualService`	N/A	N/A
	`AWS::AppMesh::VirtualGateway`	N/A	N/A
	`AWS::AppMesh::VirtualRouter`	N/A	N/A
	`AWS::AppMesh::Route`	N/A	N/A
	`AWS::AppMesh::GatewayRoute`	N/A	N/A
	`AWS::AppMesh::Mesh`	N/A	N/A

AWS AppSync

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS AppSync	`AWS::AppSync::GraphQLApi`	N/A	N/A

AWS Audit Manager

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Audit Manager	`AWS::AuditManager::Assessment`	N/A	N/A

AWS Auto Scaling

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	contains	Instancia de Amazon EC2
		está asociado a	Equilibrador de carga clásico
			Configuración de lanzamiento de Auto Scaling
			Subred
	`AWS::AutoScaling::LaunchConfiguration`	está asociado a	Grupo de seguridad de Amazon EC2
	`AWS::AutoScaling::ScalingPolicy`	está asociado a	Grupo de escalado automático
			Alarma
	`AWS::AutoScaling::`	está asociado a	Grupo de escalado automático

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`Scheduled Action`		
	`AWS::Auto Scaling:: WarmPool`	N/A	N/A

AWS Intercambio de datos B2B

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Intercambio de datos B2B	`AWS::B2BI ::Capability`	N/A	N/A

AWS Backup

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Backup	`AWS::Back up::BackupPlan`	N/D	N/A*
	`AWS::Back up::Backu pSelection`	N/A	N/A
	`AWS::Back up::Backu pVault`	N/A	N/A*

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::Backup::RecoveryPoint`	N/A	N/A
	`AWS::Backup::ReportPlan`	N/A	N/A
	`AWS::Backup::RestoreTestingPlan`	Na	N/A
AWS Backup Gateway	`AWS::BackupGateway::Hypervisor`	N/A	N/A

Debido a su AWS Backup funcionamiento, algunos de estos tipos de recursos se relacionan con los demás tipos de AWS Backup recursos de esta tabla.

`AWS::Backup::BackupPlan`está relacionado con los `AWS::Backup::BackupSelection` lugares en los que un Plan de Backup tiene muchas opciones y `AWS::Backup::BackupVault` está relacionado con los `AWS::Backup::RecoveryPoint` lugares en los que un AWS Backup Vault tiene varios puntos de recuperación.

Para obtener más información, consulte Administración de copias de seguridad mediante planes de copia de seguridad y Trabajar con almacenes de copia de seguridad.

AWS Batch

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Batch	`AWS::Batch::JobQueue`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::Batch::ComputeEnvironment`	N/A	N/A
	`AWS::Batch::SchedulingPolicy`	N/A	N/A

Administración de facturación y costos de AWS

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Administración de facturación y costos de AWS	`AWS::BCMDataExports::Export`	N/A	N/A

AWS Budgets

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Budgets	`AWS::Budgets::BudgetsAction`	N/A	N/A

AWS Certificate Manager

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Certificate Manager	`AWS::ACM::Certificate`	N/A	N/A

AWS Salas limpias

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Salas limpias ML	`AWS::CleanRoomsML::TrainingDataset`	N/A	N/A

AWS CloudFormation

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
CloudFormation	`AWS::CloudFormation::GuardHook`	N/A	N/A
	`AWS::CloudFormation::LambdaHook`	N/A	N/A
	`AWS::CloudFormation::Stack` *	contains	Tipos AWS de recursos compatibles

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::CloudFormation::StackSet`	N/A	N/A

*AWS Config registra los cambios de configuración en las CloudFormation pilas y los tipos de recursos compatibles en las pilas. AWS Config no registra los cambios de configuración de los tipos de recursos de la pila que aún no son compatibles. Los tipos de recursos no admitidos aparecerán en la sección de configuración complementaria del elemento de configuración de la pila.

AWS CloudTrail

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS CloudTrail	`AWS::CloudTrail::Trail`	N/A	N/A
	`AWS::CloudTrail::EventDataStore`	N/A	N/A

AWS Cloud9

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Cloud9	`AWS::Cloud9::EnvironmentEC2`	N/A	N/A

> **AWS Cloud9 el acceso ya no está disponible para los nuevos usuarios**
>
> Tras considerarlo detenidamente, hemos tomado la decisión de cerrar el acceso de nuevos clientes a AWS Cloud9 partir del 25 de julio de 2024. AWS Cloud9 los clientes actuales pueden seguir utilizando el servicio con normalidad. AWS sigue invirtiendo en mejoras de seguridad, disponibilidad y rendimiento AWS Cloud9, pero no tenemos previsto introducir nuevas funciones. Para obtener más información, consulte Cómo migrar de los kits de herramientas del AWS IDE AWS Cloud9 a los kits de herramientas IDE o AWS CloudShell.

AWS Cloud Map

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Detección de servicios	`AWS::ServiceDiscovery::Service`	N/A	N/A
	`AWS::ServiceDiscovery::PublicDnsNamespace`	N/A	N/A
	`AWS::ServiceDiscovery::HttpNamespace`	N/A	N/A
`AWS::ServiceDiscovery::Instance`	N/A	N/A	

AWS CodeArtifact

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	N/A	N/A
	`AWS::CodeArtifact::Domain`	N/A	N/A

AWS CodeBuild

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS CodeBuild	`AWS::CodeBuild::Project` *	está asociado a	Bucket de S3
			rol de IAM
	`AWS::CodeBuild::ReportGroup`	N/A	N/A

* Para obtener más información sobre cómo AWS Config se integra con AWS CodeBuild, consulte Usar AWS Config con AWS CodeBuild Sample.

AWS CodeDeploy

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS CodeDeploy	`AWS::CodeDeploy::Application`	contains	DeploymentGroup
	`AWS::CodeDeploy::DeploymentConfig`	N/A	N/A
	`AWS::CodeDeploy::DeploymentGroup`	está incluido en	Aplicación

AWS CodePipeline

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS CodePipeline	`AWS::CodePipeline::Pipeline` *	está conectado a	S3 bucket
		está asociado a	rol de IAM
			Proyecto de código
			Función de Lambda
			Pila de CloudFormation
			ElasticBeanstalk aplicación

*AWS Config registra los cambios de configuración de CodePipeline las canalizaciones y los tipos de recursos compatibles en las canalizaciones. AWS Config no registra los cambios de configuración de los tipos de recursos de las canalizaciones que aún no son compatibles. Los tipos de recursos no admitidos como `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, y `ECS service` aparecerán en la sección de configuración complementaria del elemento de configuración de la pila.

AWS Config

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Config	`AWS::Config::AggregationAuthorization`	N/A	N/A
	`AWS::Config::ResourceCompliance` *	está asociado a	Todos los recursos*
	`AWS::Config::ConformancePackCompliance`	N/A	N/A
	`AWS::Config::ConfigurationRecorder` *	N/A	N/A
	`AWS::Config::ConformancePack`	N/A	N/A
	`AWS::Config::StoredQuery`	N/A	N/A

*La relación entre `AWS::Config::ResourceCompliance` y un recurso relacionado depende de la forma en que `AWS::Config::ResourceCompliance` notifique la conformidad de ese tipo de recurso específico.

* `AWS::Config::ConfigurationRecorder` es un tipo de recurso del sistema AWS Config y el registro de este tipo de recurso está activado de forma predeterminada.

> **Note**
>
> El registro de los tipos de recurso `AWS::Config::ConformancePackCompliance` y `AWS::Config::ConfigurationRecorder` no tiene costo adicional.

AWS Database Migration Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Database Migration Service	`AWS::DMS::EventSubscription`	N/A	N/A
	`AWS::DMS::ReplicationSubnetGroup`	N/A	N/A
	`AWS::DMS::ReplicationInstance`	N/A	N/A
	`AWS::DMS::ReplicationTask`	N/A	N/A
	`AWS::DMS::Certificate`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::DMS::Endpoint`	N/A	N/A

AWS DataSync

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS DataSync	`AWS::DataSync::Agent`	N/A	N/A
	`AWS::DataSync::LocationSMB`	N/A	N/A
	`AWS::DataSync::LocationFSxLustre`	N/A	N/A
	`AWS::DataSync::LocationFSxWindows`	N/A	N/A
	`AWS::DataSync::LocationS3`	N/A	N/A
	`AWS::DataSync::LocationEFS`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::DataSync::LocationNFS`	N/A	N/A
	`AWS::DataSync::LocationHDFS`	N/A	N/A
	`AWS::DataSync::LocationObjectStorage`	N/A	N/A
	`AWS::DataSync::Task`	N/A	N/A

AWS Deadline Cloud

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Deadline Cloud	`AWS::Deadline::Fleet`	N/A	N/A
	`AWS::Deadline::Monitor`	N/A	N/A
	`AWS::Deadline::QueueFleetAssociation`	N/A	N/A

AWS Device Farm

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Device Farm	`AWS::DeviceFarm::TestGridProject`	N/A	N/A
	`AWS::DeviceFarm::InstanceProfile`	N/A	N/A
	`AWS::DeviceFarm::Project`	N/A	N/A

AWS Elastic Beanstalk

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Application`	contains	Versión de la aplicación Elastic Beanstalk
			Entorno de Elastic Beanstalk
		está asociado a	rol de IAM
	`AWS::ElasticBeanstalk::ApplicationVersion`	está incluido en	Aplicación Elastic Beanstalk
		está asociado a	Entorno de Elastic Beanstalk

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
			Bucket de S3
	`AWS::ElasticBeanstalk::Environment`	está incluido en	Aplicación Elastic Beanstalk
		está asociado a	Versión de la aplicación Elastic Beanstalk
			rol de IAM
		contains	CloudFormation Pila

AWS Entity Resolution

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Entity Resolution	`AWS::EntityResolution::IdMappingWorkflow`	N/A	N/A
	`AWS::EntityResolution::MatchingWorkflow`	N/A	N/A
	`AWS::EntityResolution::SchemaMapping`	N/A	N/A

AWS Fault Injection Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Fault Injection Service	`AWS::FIS::ExperimentTemplate`	N/A	N/A

AWS Global Accelerator

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	N/A	N/A
	`AWS::GlobalAccelerator::EndpointGroup`	N/A	N/A
	`AWS::GlobalAccelerator::Accelerator`	N/A	N/A

AWS Glue

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Glue	`AWS::Glue::Job`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::Glue::Classifier`	N/A	N/A
	`AWS::Glue::MLTransform`	N/A	N/A
	`AWS::Glue::Database`	N/A	N/A
	`AWS::Glue::Registry`	N/A	N/A

AWS Ground Station

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Ground Station	`AWS::GroundStation::Config`	N/A	N/A
	`AWS::GroundStation::MissionProfile`	N/A	N/A
	`AWS::GroundStation::DataflowEndpointGroup`	N/A	N/A

AWS HealthLake

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS HealthLake	`AWS::HealthLake::FHIRDatastore`	N/A	N/A

AWS Identity and Access Management (IAM)

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Identity and Access Management	`AWS::IAM::User`	está conectado a	Grupo de IAM
			Política administrada por el cliente de IAM
	`AWS::IAM::Group`	contains	Usuario de IAM
		está conectado a	Política administrada por el cliente de IAM
	`AWS::IAM::Role`	está conectado a	Política administrada por el cliente de IAM
	`AWS::IAM::Policy`	está conectado a	Usuario de IAM
			Grupo de IAM
			rol de IAM
	`AWS::IAM::SAMLProvider`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::IAM::ServerCertificate`	N/A	N/A
	`AWS::IAM::InstanceProfile`	N/A	N/A
	`AWS::IAM::OIDCProvider`	N/A	N/A
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	N/A	N/A
AWS Identity and Access Management Funciones en cualquier lugar	`AWS::RolesAnywhere::Profile`	N/A	N/A
	`AWS::RolesAnywhere::CRL`	N/A	N/A
	`AWS::RolesAnywhere::TrustAnchor`	N/A	N/A

AWS Config incluye políticas en línea con los detalles de configuración que registra. Para obtener más información sobre las políticas insertadas, consulte Políticas administradas e insertadas en la Guía del usuario de IAM.

AWS IoT

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS IoT	`AWS::IoT::AccountAuditConfiguration`	N/A	N/A
	`AWS::IoT::Authorizer`	N/A	N/A
	`AWS::IoT::CACertificate`	N/A	N/A
	`AWS::IoT::CustomMetric`	N/A	N/A
	`AWS::IoT::Dimension`	N/A	N/A
	`AWS::IoT::DomainConfiguration`	N/A	N/A
	`AWS::IoT::JobTemplate`	N/A	N/A
	`AWS::IoT::MitigationAction`	N/A	N/A
	`AWS::IoT::Policy`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::IoT::ProvisioningTemplate`	N/A	N/A
	`AWS::IoT::RoleAlias`	N/A	N/A
	`AWS::IoT::ScheduledAudit`	N/A	N/A
	`AWS::IoT::SecurityProfile`	N/A	N/A
	`AWS::IoT::ThingGroup`	N/A	N/A
	`AWS::IoTSiteWise::Gateway`	N/A	N/A
AWS IoT Wireless	`AWS::IoTWireless::ServiceProfile`	N/A	N/A
	`AWS::IoTWireless::MulticastGroup`	N/A	N/A
	`AWS::IoTWireless::FuotaTask`	N/A	N/A
AWS IoT Core	`AWS::IoT::FleetMetric`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS IoT Core Asesor de dispositivos	`AWS::IoTCoreDeviceAdvisor::SuiteDefinition`	N/A	N/A
AWS IoT Analytics	`AWS::IoTAnalytics::Datastore`	N/A	N/A
	`AWS::IoTAnalytics::Dataset`	N/A	N/A
	`AWS::IoTAnalytics::Pipeline`	N/A	N/A
	`AWS::IoTAnalytics::Channel`	N/A	N/A
AWS IoT Events	`AWS::IoTEvents::Input`	N/A	N/A
	`AWS::IoTEvents::DetectorModel`	N/A	N/A
	`AWS::IoTEvents::AlarmModel`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`	N/A	N/A
	`AWS::IoTTwinMaker::Entity`	N/A	N/A
	`AWS::IoTTwinMaker::Scene`	N/A	N/A
	`AWS::IoTTwinMaker::SyncJob`	N/A	N/A
	`AWS::IoTTwinMaker::ComponentType`	N/A	N/A
AWS IoT SiteWise	`AWS::IoTSiteWise::Asset`	N/A	N/A
	`AWS::IoTSiteWise::AssetModel`	N/A	N/A
	`AWS::IoTSiteWise::Dashboard`	N/A	N/A
	`AWS::IoTSiteWise::Portal`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::IoTSiteWise::Project`	N/A	N/A
AWS IoT Greengrass Version 2	`AWS::GreengrassV2::ComponentVersion`	N/A	N/A

AWS Key Management Service

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Key Management Service	`AWS::KMS::Key`	N/A	N/A
	`AWS::KMS::Alias`	N/A	N/A

AWS Lambda

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Lambda	`AWS::Lambda::Function`	está asociado a	rol de IAM
			Grupo de seguridad de EC2
		está incluido en	Subred EC2
	`AWS::Lambda::CodeSigningConfig`	N/A	N/A

AWS Mainframe Modernization

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Mainframe Modernization	`AWS::M2::Environment`	N/A	N/A

AWS Network Firewall

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	está conectado a	Subred EC2
		está asociado a	NetworkFirewall FirewallPolicy
	`AWS::NetworkFirewall::FirewallPolicy`	está asociado a	NetworkFirewall RuleGroup
	`AWS::NetworkFirewall::RuleGroup`	N/A	N/A
	`AWS::NetworkFirewall::TLSInspectionConfiguration`	N/A	N/A
	`AWS::NetworkFirewall::VpcEn`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`dpointAssociation`		

AWS Network Manager

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Network Manager	`AWS::NetworkManager::TransitGatewayRegistration`	N/A	N/A
	`AWS::NetworkManager::Site`	N/A	N/A
	`AWS::NetworkManager::Device`	N/A	N/A
	`AWS::NetworkManager::Link`	N/A	N/A
	`AWS::NetworkManager::GlobalNetwork`	N/A	N/A
	`AWS::NetworkManager::Custom`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`erGateway Association`		
	`AWS::NetworkManager::LinkAssociation`	N/A	N/A
	`AWS::NetworkManager::ConnectPeer`	N/A	N/A
	`AWS::NetworkManager::TransitGatewayPeering`	N/A	N/A

AWS Organizations

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Organizations	`AWS::Organizations::OrganizationalUnit`	N/A	N/A

AWS Panorama

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Panorama	`AWS::Panorama::Package`	N/A	N/A

AWS Private Certificate Authority

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`	N/A	N/A
	`AWS::ACMPCA::CertificateAuthorityActivation`	N/A	N/A
Autoridad de certificación privada de AWS Conector para Active Directory	`AWS::PCAConnectorAD::Connector`	N/A	N/A
	`AWS::PCAConnectorAD::DirectoryRegistration`	N/A	N/A

AWS Resilience Hub

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Resilience Hub	`AWS::ResilienceHub::ResiliencyPolicy`	N/A	N/A
	`AWS::ResilienceHub::App`	N/A	N/A

Explorador de recursos de AWS

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Explorador de recursos de AWS	`AWS::ResourceExplorer2::Index`	N/A	N/A

AWS RoboMaker

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS RoboMaker	`AWS::RoboMaker::RobotApplicationVersion`	N/A	N/A
	`AWS::RoboMaker::RobotApplication`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::RoboMaker::SimulationApplication`	N/A	N/A

AWS Signer

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Signer	`AWS::Signer::SigningProfile`	N/A	N/A

AWS Secrets Manager

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Secrets Manager	`AWS::SecretsManager::Secret`	está asociado a	Lambda function
		está asociado a	Clave de KMS
	`AWS::SecretsManager::ResourcePolicy`	N/A	N/A
	`AWS::SecretsManager::RotationSchedule`	N/A	N/A

AWS Security Hub CSPM

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Security Hub CSPM	`AWS::SecurityHub::Standard`	N/A	N/A

AWS Service Catalog

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Service Catalog	`AWS::ServiceCatalog::CloudFormationProduct`	está incluido en	Portfolio
		está asociado a	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationProvisionedProduct`	está asociado a	Portafolio
			CloudFormationProduct
			CloudFormationStack
	`AWS::ServiceCatalog::Portfolio`	contains	CloudFormationProduct

> **Note**
>
> Cuando se usa AWS Service Catalog with AWS Config, los elementos de configuración muestran el ARN del producto aprovisionado secundario en lugar del ARN del producto

principal. Esto ocurre cuando un producto AWS Service Catalog aprovisionado sirve como recurso dentro de un producto aprovisionado principal de forma continua. CloudFormation El ID del recurso sigue siendo rastreable a través de las interfaces. AWS Config

AWS Shield

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Shield	`AWS::Shield::Protection`	está asociado a	CloudFront Distribución en Amazon
	`AWS::ShieldRegional::Protection`	está asociado a	EC2 EIP
		está asociado a	ElasticLoadBalancing Equilibrador
		está asociado a	ElasticLoadBalancingV2 LoadBalancer

AWS Step Functions

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Step Functions	`AWS::StepFunctions::Activity`	N/A	N/A
	`AWS::StepFunctions::StateMachine`	N/A	N/A

AWS Systems Manager

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Systems Manager	`AWS::SSM::ManagedInstanceInventory` *	está asociado a	Instancia de EC2
	`AWS::SSM::PatchCompliance`	está asociado a	Inventario de instancias administradas
	`AWS::SSM::AssociationCompliance`	está asociado a	Inventario de instancias administradas
	`AWS::SSM::FileData`	está asociado a	Inventario de instancias administradas
	`AWS::SSM::Document`	N/A	N/A
	`AWS::SSM::ResourceDataSync`	N/A	N/A
Administrador de incidentes de AWS Systems Manager	`AWS::SSMIncidents::ResponsePlan`	N/A	N/A
Administrador de incidentes de AWS Systems Manager Contactos	`AWS::SSMContacts::Contact`	N/A	N/A

*Para obtener más información sobre el inventario de instancias administradas, consulte Recording Software Configuration for Managed Instances.

AWS Transfer Family

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Transfer Family	`AWS::Transfer::Agreement`	N/A	N/A
	`AWS::Transfer::Connector`	N/A	N/A
	`AWS::Transfer::Workflow`	N/A	N/A
	`AWS::Transfer::Certificate`	N/A	N/A
	`AWS::Transfer::Profile`	N/A	N/A
	`AWS::Transfer::Server`	N/A	N/A

AWS WAF

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS WAF	`AWS::WAF::RateBasedRule`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::WAF::Rule`	N/A	N/A
	`AWS::WAF::WebACL`	está asociado a	Regla de WAF
			Regla basada en frecuencia de WAF
			Grupo de reglas de WAF
	`AWS::WAF::RuleGroup`	está asociado a	Regla de WAF
	`AWS::WAFRegional::RateBasedRule`	N/A	N/A
	`AWS::WAFRegional::Rule`	N/A	N/A
	`AWS::WAFRegional::WebACL`	está asociado a	ElasticLoadBalancingV2 LoadBalancer
			WAFRegional Regla
			WAFRegional regla basada en la tarifa
			WAFRegional Grupo de reglas
	`AWS::WAFRegional::RuleGroup`	está asociado a	WAFRegional Regla
AWS WAF V2	`AWS::WAFv2::WebACL`	está asociado a	ElasticLoadBalancingV2 LoadBalancer

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
			ApiGateway Escenario
			WAFv2 IPSet
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup
			WAFv2 ManagedRuleSet
	`AWS::WAFv2::RuleGroup`	está asociado a	WAFv2 IPSet
			WAFv2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	está asociado a	WAFv2 RuleGroup
	`AWS::WAFv2::IPSet`	N/A	N/A
	`AWS::WAFv2::RegexPatternSet`	N/A	N/A

AWS X-Ray

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS X-Ray	`AWS::XRay::EncryptionConfig`	N/A	N/A

Elastic Load Balancing

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
Elastic Load Balancing	Equilibrador de carga de aplicación	está asociado a	Grupo de seguridad de EC2
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	está conectado a	Subred
		está incluido en	Nube privada virtual (VPC)
	Cuadro de diálogo del oyente del equilibrador de carga de aplicación `AWS::ElasticLoadBalancingV2::Listener`	N/A	N/A
	Grupo objetivo de Application Load Balancer	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`AWS::ElasticLoadBalancingV2::TargetGroup`		
	Equilibrador de carga clásico `AWS::ElasticLoadBalancing::LoadBalancer`	está asociado a	Grupo de seguridad de EC2
		está conectado a	Subred
		está incluido en	Nube privada virtual (VPC)
	Equilibrador de carga de red `AWS::ElasticLoadBalancingV2::LoadBalancer`	N/A	N/A

AWS Elemental MediaConnect

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Elemental MediaConnect	`AWS::MediaConnect::FlowEntitlement`	N/A	N/A
	`AWS::MediaConnect:`	N/A	N/A

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
	`:FlowVpcInterface`		
	`AWS::MediaConnect::FlowSource`	N/A	N/A
	`AWS::MediaConnect::Gateway`	N/A	N/A

AWS Elemental MediaPackage

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Elemental MediaPackage	`AWS::MediaPackage::PackagingGroup`	N/A	N/A
	`AWS::MediaPackage::PackagingConfiguration`	N/A	N/A

AWS Elemental MediaPackage V2

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Elemental MediaPackage V2	`AWS::MediaPackageV2::Channel`	N/A	N/A
	`AWS::MediaPackageV2::ChannelGroup`	N/A	N/A
	`AWS::MediaPackageV2::OriginEndpoint`	N/A	N/A

AWS Elemental MediaTailor

AWS Servicio	Valor de tipo de recurso	Relación	Recurso relacionado
AWS Elemental MediaTailor	`AWS::MediaTailor::LiveSource`	N/A	N/A
	`AWS::MediaTailor::PlaybackConfiguration`	N/A	N/A

Cobertura de los recursos según la disponibilidad por región

Regiones de América del Norte y del Sur

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::ACM::Certificate	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ACMPCA::CertificateAuthority	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ACMPCA::CertificateAuthorityActivación	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::APS::RuleGroupsEspacio de nombres	No	Sí	Sí	Sí	No	No	Sí	Sí
AWS::AccessAnalyzer::Analyzer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AmazonMQ::Broker	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Amplify::App	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Amplify::Branch	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ApiGateway::DomainName	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::ApiGateway::Method	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGateway::RestApi	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGateway::Stage	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGateway::UsagePlan	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Api	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Integration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Stage	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppConfig::Application	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppConfig::ConfigurationProfile	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppConfig::DeploymentStrategy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppConfig::Environment	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::AppConfig::Extension	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppConfig::ExtensionAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppConfig::HostedConfigurationVersión	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppFlow::Flow	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppIntegrations::Application	No	Sí	Sí	No	No	Sí	No	No
AWS::AppIntegrations::DataIntegration	No	Sí	Sí	No	No	Sí	No	No
AWS::AppIntegrations::EventIntegration	No	Sí	Sí	No	No	Sí	No	No
AWS::AppMesh::GatewayRoute	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppMesh::Mesh	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppMesh::Route	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppMesh::VirtualGateway	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::AppMesh::VirtualNode	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppMesh::VirtualRouter	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppMesh::VirtualService	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppRunner::Service	No	Sí	Sí	Sí	No	No	No	No
AWS::AppRunner::VpcConnector	No	Sí	Sí	Sí	No	No	No	No
AWS::AppStream::AppBlockConstructor	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppStream::Application	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppStream::DirectoryConfig	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppStream::Fleet	No	Sí	Sí	Sí	No	Sí	No	No
AWS::AppStream::Stack	No	Sí	Sí	Sí	No	Sí	No	No
AWS::AppSync::Api	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::AppSync::ApiCache	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::AppSync::GraphQLApi	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Athena::DataCatalog	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Athena::PreparedStatement	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Athena::WorkGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AuditManager::Assessment	Sí	Sí	Sí	Sí	No	Sí	No	No
AWS::AutoScaling::AutoScalingGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::LaunchConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::ScalingPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::ScheduledAction	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::WarmPool	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::B2BI::Capability	No	Sí	Sí	Sí	No	No	No	No
AWS::B2BI::Profile	No	Sí	Sí	Sí	No	No	No	No
AWS::BCMDataExports::Export	No	Sí	No	No	No	No	No	No
AWS::Backup::BackupPlan	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Backup::BackupSelection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Backup::BackupVault	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Backup::RecoveryPoint	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::Backup::ReportPlan	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Backup::RestoreTestingPlan	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::BackupGateway::Hypervisor	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Batch::ComputeEnvironment	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Batch::JobQueue	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Batch::SchedulingPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Perfil de AWS::Bedrock::ApplicationInference	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Bedrock::Guardrail	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Bedrock::KnowledgeBase	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Bedrock::Prompt	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::BedrockAgentCore::BrowserCustom	No	Sí	Sí	Sí	No	No	No	No
AWS::BedrockAgentCore::CodeInterpreterPersonalizado	No	Sí	Sí	Sí	No	No	No	No
AWS::BedrockAgentCore::Runtime	No	Sí	Sí	Sí	No	No	No	No
AWS::Budgets::BudgetsAction	No	Sí	No	No	No	No	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Cassandra::Keyspace	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::CleanRoomsML::TrainingDataset	No	Sí	Sí	Sí	No	No	No	No
AWS::Cloud9::EnvironmentEC2	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::CloudFormation::GuardHook	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudFormation::LambdaHook	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudFormation::Stack	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudFormation::StackSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudFront::Distribution	No	Sí	No	No	No	No	No	No
AWS::CloudFront::KeyValueTienda	No	Sí	No	No	No	No	No	No
AWS::CloudFront::PublicKey	No	Sí	No	No	No	No	No	No
AWS::CloudFront::RealtimeLogConfig	No	Sí	No	No	No	No	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::CloudFront::StreamingDistribution	No	Sí	No	No	No	No	No	No
AWS::CloudTrail::EventDataTienda	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::CloudTrail::Trail	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudWatch::Alarm	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudWatch::MetricStream	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::CodeArtifact::Domain	No	Sí	Sí	Sí	No	No	No	No
AWS::CodeArtifact::Repository	No	Sí	Sí	Sí	No	No	No	No
AWS::CodeBuild::Project	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::CodeBuild::ReportGroup	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::CodeDeploy::Application	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::CodeDeploy::DeploymentConfig	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::CodeDeploy::DeploymentGroup	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::CodeGuruProfiler::ProfilingGroup	No	Sí	Sí	Sí	No	No	No	No
AWS::CodeGuruReviewer::RepositoryAssociation	No	Sí	Sí	Sí	No	No	No	No
AWS::CodePipeline::Pipeline	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Cognito::IdentityPool	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Cognito::UserPool	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Cognito::UserPoolCliente	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Cognito::UserPoolGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Comprehend::Flywheel	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Config::AggregationAuthorization	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Config::ConfigurationRecorder	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Config::ConformancePack	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
Conformidad de AWS::Config::ConformancePack	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::Config::ResourceCompliance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Config::StoredQuery	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Connect::Instance	No	Sí	Sí	No	No	Sí	No	No
AWS::Connect::PhoneNumber	No	Sí	Sí	No	No	Sí	No	No
AWS::Connect::QuickConnect	No	Sí	Sí	No	No	Sí	No	No
AWS::Connect::Rule	No	Sí	Sí	No	No	Sí	No	No
AWS::Connect::SecurityProfile	No	Sí	Sí	No	No	Sí	No	No
AWS::Connect::User	No	Sí	Sí	No	No	Sí	No	No
AWS::CustomerProfiles::Domain	No	Sí	Sí	No	No	Sí	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::CustomerProfiles::ObjectType	No	Sí	Sí	No	No	Sí	No	No
AWS::DMS::Certificate	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::DMS::Endpoint	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::DMS::EventSubscription	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::DMS::MigrationProject	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::DMS::ReplicationInstance	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::DMS::ReplicationSubnetGrupo	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::DMS::ReplicationTask	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::DataSync::Agent	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::LocationEFS	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::DataSync::LocationFSxLustre	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::DataSync::LocationFSxVentanas	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::DataSync::LocationHDFS	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::DataSync::LocationNFS	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::DataSync::LocationObjectAlmacenamiento	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::DataSync::LocationS3	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::LocationSMB	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::DataSync::Task	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Deadline::Fleet	No	Sí	Sí	Sí	No	No	No	No
AWS::Deadline::Monitor	No	Sí	Sí	Sí	No	No	No	No
AWS::Deadline::QueueFleetAsociación	No	Sí	Sí	Sí	No	No	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Detective::Graph	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::DeviceFarm::InstanceProfile	No	No	Sí	No	No	No	No	No
AWS::DeviceFarm::Project	No	No	Sí	No	No	No	No	No
AWS::DeviceFarm::TestGridProyecto	No	No	Sí	No	No	No	No	No
AWS::DynamoDB::Table	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Capacity Reservation	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::EC2::CarrierGateway	No	Sí	Sí	Sí	No	Sí	No	No
AWS::EC2::ClientVpnPunto final	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EC2::ClientVpnTargetNetworkAssociation	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EC2::CustomerGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: DHCPOptions	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::EC2: EC2 Flota	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS:EC2: :EIP	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: EIPAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::EgressOnlyInternetGateway	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EC2::FlowLog	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Host	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2: :IPAM	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS:EC2:: IPAMPool	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS:EC2: IPAMPool Cir	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::EC2: IPAMResource Descubrimiento	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS:EC2:: IPAMResource DiscoveryAssociation	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS:EC2:: IPAMScope	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EC2::Instance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Instance ConnectPunto final	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2: :InternetGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2: :LaunchTemplate	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EC2::NatGateway	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EC2::NetworkAcl	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::NetworkInsightsAccessScope	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::EC2: :NetworkInsightsAccessScopeAnalysis	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::EC2::NetworkInsightsAnálisis	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::EC2::NetworkInsightsRuta	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::EC2::NetworkInterface	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::PrefixList	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::RouteTable	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SecurityGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SecurityGroupVpcAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SnapshotBlockPublicAccess	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SpotFleet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Subnet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SubnetCidrBloquear	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SubnetNetworkAclAssociation	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::EC2::SubnetRouteTableAssociation	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::EC2::TrafficMirrorFiltro	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::TrafficMirrorSession	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::EC2::TrafficMirrorObjetivo	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::EC2::TransitGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::TransitGatewayAdjunto	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EC2::TransitGatewayConnect	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EC2::TransitGatewayMulticastDomain	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::TransitGatewayRouteTable	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS:EC2: :VPC	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCBlockPublicAccessExclusion	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS:EC2:: VPCBlock PublicAccessOptions	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS:EC2:: VPCEndpoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCEndpoint ConnectionNotification	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCEndpoint Servicio	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCGateway Adjunto	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCPeering Conexión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPNConnection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPNConnection Ruta	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPNGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Verified AccessInstancia	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EC2::Volume	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::ECR::PublicRepository	No	Sí	No	No	No	No	No	No
AWS::ECR::PullThroughCacheRule	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::RegistryPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::ReplicationConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::Repository	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::RepositoryCreationPlantilla	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::CapacityProvider	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::Cluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::Service	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::TaskDefinition	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::TaskSet	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::EFS::AccessPoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EFS::FileSystem	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EKS::Addon	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EKS::Cluster	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::EKS::FargateProfile	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EKS::Identity ProviderConfig	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EMR::Security Configuration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EMR::Studio	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::EMRContainers ::VirtualCluster	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EMRS erverless::Application	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ElasticBeanst alk::Application	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::ElasticBeanstalk::ApplicationVersion	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::ElasticBeanstalk::Environment	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::ElasticLoadBalancing::LoadBalancer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ElasticLoadBalancingV2::Listener	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::ElasticLoadBalancingV2::LoadBalancer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ElasticLoadBalancingV2::TargetGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Elasticsearch::Domain	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EntityResolution::IdMappingflujo de trabajo	No	Sí	Sí	Sí	No	Sí	No	No
AWS::EntityResolution::MatchingWorkflow	No	Sí	Sí	Sí	No	Sí	No	No
AWS::EntityResolution::SchemaMapping	No	Sí	Sí	Sí	No	Sí	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::EventSchemas::Discoverer	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EventSchemas::Registry	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EventSchemas::RegistryPolicy	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::EventSchemas::Schema	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Events::ApiDestination	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Events::Archive	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Events::Connection	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Events::Endpoint	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Events::EventBus	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Events::Rule	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::FIS::ExperimentTemplate	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Forecast::Dataset	No	Sí	Sí	Sí	No	No	No	No
AWS::Forecast::DatasetGroup	No	Sí	Sí	Sí	No	No	No	No
AWS::FraudDetector::EntityType	No	Sí	Sí	Sí	No	No	No	No
AWS::FraudDetector::Label	No	Sí	Sí	Sí	No	No	No	No
AWS::FraudDetector::Outcome	No	Sí	Sí	Sí	No	No	No	No
AWS::FraudDetector::Variable	No	Sí	Sí	Sí	No	No	No	No
AWS::GameLift::Alias	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::GameLift::Build	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::GameLift::GameSessionCola	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::GameLift::MatchmakingConfiguration	No	Sí	Sí	No	No	No	No	No
AWS::GlobalAccelerator::Accelerator	No	No	Sí	No	No	No	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::GlobalAccelerator::EndpointGroup	No	No	Sí	No	No	No	No	No
AWS::GlobalAccelerator::Listener	No	No	Sí	No	No	No	No	No
AWS::Glue::Classifier	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Glue::Database	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Glue::Job	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::Glue::MLTransform	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Glue::Registry	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Grafana::Workspace	No	Sí	Sí	Sí	No	No	No	No
AWS::GreengrassV2::ComponentVersion	No	Sí	Sí	Sí	No	Sí	No	No
AWS::GroundStation::Config	No	Sí	Sí	Sí	No	No	No	Sí
AWS::GroundStation::DataflowEndpointGrupo	No	Sí	Sí	Sí	No	No	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::GroundStation ::MissionProfile	No	Sí	Sí	Sí	No	No	No	Sí
AWS::GuardDuty::Detector	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::GuardDuty::Filter	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::GuardDeber: IPSet	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::GuardDuty::Ma lwareProtectionPlan	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::GuardDuty::Th reatIntelSet	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::HealthLago: FHIRDatastore	No	Sí	Sí	Sí	No	No	No	No
AWS::IAM::Group	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IAM::InstanceProfile	No	Sí	No	No	No	No	No	No
AWS: :IAM: OIDCProvider	No	Sí	No	No	No	No	No	No
AWS::IAM::Policy	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::IAM::Role	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS: :IAM: SAMLProvider	No	Sí	No	No	No	No	No	No
AWS::IAM: :ServerCertificate	No	Sí	No	No	No	No	No	No
AWS::IAM::User	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IVS::Channel	No	Sí	Sí	No	No	No	No	No
AWS::IVS::PlaybackKeyPar	No	Sí	Sí	No	No	No	No	No
AWS::IVS::RecordingConfiguration	No	Sí	Sí	No	No	No	No	No
AWS::ImageBuilder: :ContainerRecipe	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ImageBuilder: :DistributionConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ImageBuilder: :ImagePipeline	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ImageBuilder: :ImageRecipe	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::ImageBuilder::InfrastructureConfiguration	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ImageBuilder::LifecyclePolicy	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::InspectorV2::Activation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::InspectorV2::Filter	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::IoT::AccountAuditConfiguración	Sí	Sí	Sí	Sí	No	Sí	No	No
AWS::IoT::Authorizer	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IoT:: CACertificate	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IoT::CustomMetric	Sí	Sí	Sí	Sí	No	Sí	No	No
AWS::IoT::Dimension	Sí	Sí	Sí	Sí	No	Sí	No	No
AWS::IoT::DomainConfiguration	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IoT::FleetMetric	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::IoT::JobTemplate	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IoT::MitigationAction	Sí	Sí	Sí	Sí	No	Sí	No	No
AWS::IoT::Policy	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IoT::ProvisioningTemplate	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IoT::RoleAlias	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IoT::ScheduledAudit	Sí	Sí	Sí	Sí	No	Sí	No	No
AWS::IoT::SecurityProfile	Sí	Sí	Sí	Sí	No	Sí	No	No
AWS::IoT::ThingGroup	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::IoTAnalytics::Channel	No	Sí	Sí	Sí	No	No	No	No
AWS::IoTAnalytics::Dataset	No	Sí	Sí	Sí	No	No	No	No
AWS::IoTAnalytics::Datastore	No	Sí	Sí	Sí	No	No	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::IoTAnalytics::Pipeline	No	Sí	Sí	Sí	No	No	No	No
AWS::IoTCoreDevice Advisor::SuiteDefinition	No	Sí	Sí	No	No	No	No	No
AWS::IoTE vents::AlarmModel	No	Sí	Sí	Sí	No	Sí	No	No
AWS::IoTEvents::De tectorModel	No	Sí	Sí	Sí	No	Sí	No	No
AWS::IoTEvents::Input	No	Sí	Sí	Sí	No	Sí	No	No
AWS::IoTSiteWise::Asset	No	Sí	Sí	Sí	No	Sí	No	No
AWS::IoTSiteWise:: AssetModel	No	Sí	Sí	Sí	No	Sí	No	No
AWS::IoTS iteWise::Dashboard	No	Sí	Sí	Sí	No	Sí	No	No
AWS::IoTS iteWise::Gateway	No	Sí	Sí	Sí	No	Sí	No	No
AWS::IoTSiteWise::Portal	No	Sí	Sí	Sí	No	Sí	No	No
AWS::IoTSiteWise::Project	No	Sí	Sí	Sí	No	Sí	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::IoTTwinMaker::ComponentType	No	Sí	Sí	No	No	No	No	No
AWS::IoTTwinMaker::Entity	No	Sí	Sí	No	No	No	No	No
AWS::IoTTwinMaker::Scene	No	Sí	Sí	No	No	No	No	No
AWS::IoTTwinMaker::SyncJob	No	Sí	Sí	No	No	No	No	No
AWS::IoTTwinMaker::Workspace	No	Sí	Sí	No	No	No	No	No
AWS::IoTWireless::FuotaTask	No	Sí	Sí	No	No	No	No	Sí
AWS::IoTWireless::MulticastGroup	No	Sí	Sí	No	No	No	No	Sí
AWS::IoTWireless::ServiceProfile	No	Sí	Sí	No	No	No	No	Sí
AWS::KMS::Alias	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::KMS::Key	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::KafkaConnect::Connector	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::KafkaConnect::CustomPlugin	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::Kendra::Index	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Kinesis::Stream	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::Kinesis::StreamConsumer	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::KinesisAnalyticsV2::Application	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::KinesisFirehose::DeliveryStream	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::KinesisVideo::SignalingChannel	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::KinesisVideo::Stream	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Lambda::CodeSigningConfig	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Lambda::Function	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Lex::Bot	No	Sí	Sí	No	No	Sí	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Lex::BotAlias	No	Sí	Sí	No	No	Sí	No	No
AWS::Lightsail::Bucket	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Lightsail::Certificate	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Lightsail::Disk	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Lightsail::StaticIp	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Location::APIKey	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Location::GeofenceCollection	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Location::Map	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Location::PlaceIndex	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Location::RouteCalculator	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Logs::Destination	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::LookoutVision::Project	No	Sí	Sí	Sí	No	No	No	No
AWS::M2::Environment	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MSK::BatchScramSecreto	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MSK::Cluster	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MSK::ClusterPolicy	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MSK::Configuration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::MSK::ServerlessCluster	No	Sí	Sí	Sí	No	Sí	No	No
AWS::MSK::VpcConnection	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Macie::Session	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaConnect::FlowEntitlement	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaConnect::FlowSource	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::MediaConnect::FlowVpcInterfaz	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaConnect::Gateway	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaLive::Multiplexprogram	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaPackage::Asset	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaPackage::PackagingConfiguration	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaPackage::PackagingGroup	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaPackageV2::Channel	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaPackageV2::ChannelGroup	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaPackageV2::OriginEndpoint	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaTailor::LiveSource	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::MediaTailor::PlaybackConfiguration	No	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::MemoryDB::SubnetGroup	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::NetworkFirewall::Firewall	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::FirewallPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::RuleGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall: TLSInspection Configuración	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::VpcEndpointAsociación	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkManager::ConnectPeer	No	No	Sí	No	No	No	No	No
AWS::NetworkManager::CustomerGatewayAsociación	No	No	Sí	No	No	No	No	No
AWS::NetworkManager::Device	No	No	Sí	No	No	No	No	No
AWS::NetworkManager::GlobalNetwork	No	No	Sí	No	No	No	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::NetworkManager::Link	No	No	Sí	No	No	No	No	No
AWS::NetworkManager::LinkAssociation	No	No	Sí	No	No	No	No	No
AWS::NetworkManager::Site	No	No	Sí	No	No	No	No	No
AWS::NetworkManager::TransitGatewayPeering	No	No	Sí	No	No	No	No	No
AWS::NetworkManager::TransitGatewayRegistro	No	No	Sí	No	No	No	No	No
AWS::Omics::RunGroup	No	Sí	Sí	No	No	No	No	No
AWS::Omics::Workflow	No	Sí	Sí	No	No	No	No	No
AWS::OpenSearch::Domain	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::OpenSearchServerless::Collection	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::OpenSearchServerless::SecurityConfig	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::OpenSearchServerless::VpcEndpoint	No	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::PCAConnectorAD::Connector	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::PCAConnectorAD::DirectoryRegistration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Panorama::Package	No	Sí	Sí	No	No	Sí	No	No
AWS::Personalize::Dataset	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Personalize::DatasetGroup	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Personalize::Schema	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Personalize::Solution	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Pinpoint::App	No	Sí	Sí	No	No	Sí	No	No
AWS::Pinpoint::ApplicationSettings	No	Sí	Sí	No	No	Sí	No	No
AWS::Pinpoint::Campaign	No	Sí	Sí	No	No	Sí	No	No
AWS::Pinpoint::EmailChannel	No	Sí	Sí	No	No	Sí	No	No

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Pinpoint::EmailTemplate	No	Sí	Sí	No	No	Sí	No	No
AWS::Pinpoint::EventStream	No	Sí	Sí	No	No	Sí	No	No
AWS::Pinpoint::InAppPlantilla	No	Sí	Sí	Sí	No	Sí	No	No
AWS::Pinpoint::Segment	No	Sí	Sí	No	No	Sí	No	No
AWS::QuickSight::Dashboard	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::QuickSight::DataSource	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::QuickSight::Template	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::QuickSight::Theme	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS: :RDS: DBCluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Instantánea DBCluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS: DBInstance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS: :RDS:: Punto final DBProxy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Grupo DBSecurity	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS: DBSnapshot	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Grupo DBSubnet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RDS: :EventSubscription	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RDS::GlobalCluster	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::RDS::Integration	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::RDS::OptionGroup	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::RUM::AppMonitor	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Redshift::Cluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::Clu sterParameterGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Redshift::ClusterSecurityGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSnapshot	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSubnetGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::EndpointAccess	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Redshift::EndpointAuthorization	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Redshift::EventSubscription	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::Integration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ScheduledAction	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ResilienceHub::App	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ResilienceHub::ResiliencyPolicy	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ResourceExplorer2::Index	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::RoboMaker::RobotApplication	No	Sí	Sí	Sí	No	No	No	No
AWS::RoboMaker::RobotApplicationVersión	No	Sí	Sí	Sí	No	No	No	No
AWS::RoboMaker::SimulationApplication	No	Sí	Sí	Sí	No	No	No	No
AWS::RolesEncualquier lugar: :CRL	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RolesAnywhere::Profile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RolesAnywhere::TrustAnchor	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53: :DNSSEC	No	Sí	No	No	No	No	No	No
AWS::Route53::HealthCheck	No	Sí	No	No	No	No	No	No
AWS::Route53::HostedZone	No	Sí	No	No	No	No	No	No
AWS::Route53Profiles::Profile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Profiles::ProfileAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Route53RecoveryControl::Cluster	No	No	Sí	No	No	No	No	No
AWS::Route53RecoveryControl::ControlPanel	No	No	Sí	No	No	No	No	No
AWS::Route53RecoveryControl::RoutingControl	No	No	Sí	No	No	No	No	No
AWS::Route53RecoveryControl::SafetyRule	No	No	Sí	No	No	No	No	No
AWS::Route53RecoveryReadiness::Cell	No	No	Sí	No	No	No	No	No
AWS::Route53RecoveryReadiness::ReadinessCheck	No	No	Sí	No	No	No	No	No
AWS::Route53RecoveryReadiness::RecoveryGroup	No	No	Sí	No	No	No	No	No
AWS::Route53RecoveryReadiness::ResourceSet	No	No	Sí	No	No	No	No	No
AWS::Route53Resolver::FirewallDomainLista	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Route53Resolver::FirewallRuleGrupo	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverEndpoint	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverRule	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Route53Resolver::ResolverRuleAsociación	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::S3::AccessGrant	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::AccessGrantsInstancia	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::AccessGrantsLocation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::AccessPoint	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::S3::AccountPublicAccessBlock	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::S3::Bucket	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::MultiRegionAccessPoint	No	No	Sí	No	No	No	No	No
AWS::S3::StorageLens	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::S3::StorageLensGrupo	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::S3Express::BucketPolicy	No	Sí	Sí	Sí	No	No	No	No
AWS::S3Express::DirectoryBucket	No	Sí	Sí	Sí	No	No	No	No
AWS::S3Tables::TableBucket	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3Tables::TableBucketPolítica	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SES::ConfigurationSet	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SES::ContactList	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::SES::DedicatedIpPiscina	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SES::MailManagerTrafficPolicy	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SES::ReceiptFilter	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SES::ReceiptRuleSet	No	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SES::Template	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SNS::Topic	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SQS::Queue	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SSM::AssociationCompliance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSM::Document	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSM::FileData	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Inventario de AWS::SSM::ManagedInstance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::SSM::PatchCompliance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSM::ResourceDataSincronizar	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSMContacts::Contact	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SSMIncidents::ResponsePlan	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::AppImageConfig	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::CodeRepository	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::DataQualityJobDefinition	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::Domain	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::EndpointConfig	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::FeatureGroup	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::Image	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::SageMaker::InferenceExperiment	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::MlflowTrackingServidor	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SageMaker::Model	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::ModelBiasJobDefinition	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::ModelExplainabilityJobDefinition	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::ModelQualityJobDefinition	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::MonitoringSchedule	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::NotebookInstance	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::StudioLifecycleConfig	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::SageMaker::UserProfile	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::SageMaker::Workteam	No	Sí	Sí	Sí	No	Sí	No	No
AWS::SecretsManager::ResourcePolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SecretsManager::RotationSchedule	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SecretsManager::Secret	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SecurityHub::Standard	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ServiceCatalog::CloudFormationProducto	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ServiceCatalog::Portfolio	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ServiceDiscovery::HttpNamespace	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::ServiceDiscovery::Instance	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::ServiceDiscovery::PublicDnsEspacio de nombres	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ServiceDiscovery::Service	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::Shield::Protection	No	Sí	No	No	No	No	No	No
AWS::ShieldRegional::Protection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Signer::SigningProfile	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::Step Functions::Activity	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::StepFunctions::StateMachine	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Transfer::Agreement	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
AWS::Transfer::Certificate	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::Transfer::Connector	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Transfer::Profile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Transfer::Server	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Transfer::Workflow	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAF::RateBasedRegla	No	Sí	No	No	No	No	No	No
AWS::WAF::Rule	No	Sí	No	No	No	No	No	No
AWS::WAF::RuleGroup	No	Sí	No	No	No	No	No	No
AWS::WAF::WebACL	No	Sí	No	No	No	No	No	No
AWS::WAFRegional::RateBasedRegla	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::WAFRegional::Rule	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS::WAFRegional::RuleGroup	Sí	Sí	Sí	Sí	No	Sí	No	Sí

Tipo de recurso	EE.UU. Oeste (Norte de California)	EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Oregón)	EE.UU. Este (Ohio)	Oeste de Canadá (Calgary	Canadá (Central)	México (Central)	América del Sur (São Paulo)
AWS::WAFRegional::WebACL	Sí	Sí	Sí	Sí	No	Sí	No	Sí
AWS:WAFv2:: IPSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv2::ManagedRuleSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv2::RegexPatternSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv2::RuleGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv2::WebACL	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WorkSpaces::ConnectionAlias	No	Sí	Sí	No	No	Sí	No	Sí
AWS::WorkSpaces::Workspace	No	Sí	Sí	No	No	Sí	No	Sí
AWS::XRay::EncryptionConfig	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí

Regiones de Europa

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::ACM::Certificate	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ACMPCA::CertificateAuthority	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ACMPCA::CertificateAuthorityActivación	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::APS::RuleGroupsEspacio de nombres	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::AccessAnalyzer::Analyzer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AmazonMQ::Broker	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::Amplify::App	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::Amplify::Branch	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::ApiGateway::DomainName	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGateway::Method	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGateway::RestApi	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::ApiGateway::Stage	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGateway::UsagePlan	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Api	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Integration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Stage	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppConfig::Application	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppConfig::ConfigurationProfile	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppConfig::DeploymentStrategy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppConfig::Environment	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppConfig::Extension	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppConfig::ExtensionAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppConfig::HostedConfigurationVersión	Sí	Sí	Sí	Sí	Sí	Sí	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::AppFlow::Flow	Sí	Sí	Sí	Sí	No	No	No	No
AWS::AppIntegrations::Application	No	Sí	Sí	No	No	No	No	No
AWS::AppIntegrations::DataIntegration	No	Sí	Sí	No	No	No	No	No
AWS::AppIntegrations::EventIntegration	No	Sí	Sí	No	No	No	No	No
AWS::AppMesh::GatewayRoute	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppMesh::Mesh	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppMesh::Route	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppMesh::VirtualGateway	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppMesh::VirtualNode	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppMesh::VirtualRouter	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppMesh::VirtualService	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::AppRunner::Service	Sí	Sí	Sí	Sí	No	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::AppRunner::VpcConnector	Sí	Sí	No	Sí	No	No	No	No
AWS::AppStream::AppBlockConstructor	Sí	Sí	Sí	Sí	No	No	No	No
AWS::AppStream::Application	Sí	Sí	Sí	Sí	No	No	No	No
AWS::AppStream::DirectoryConfig	Sí	Sí	Sí	Sí	No	No	No	No
AWS::AppStream::Fleet	Sí	Sí	Sí	No	No	No	No	No
AWS::AppStream::Stack	Sí	Sí	Sí	No	No	No	No	No
AWS::AppSync::Api	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppSync::ApiCache	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AppSync::GraphQLApi	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Athena::DataCatalog	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Athena::PreparedStatement	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Athena::WorkGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::AuditManager::Assessment	Sí	Sí	Sí	No	No	No	No	No
AWS::AutoScaling::AutoScalingGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::LaunchConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::ScalingPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::ScheduledAction	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Auto Scaling::WarmPool	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::BCMDataExports::Export	No	No	Sí	No	No	No	No	No
AWS::Backup::BackupPlan	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Backup::BackupSelection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Backup::BackupVault	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Backup::RecoveryPoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Backup::ReportPlan	Sí	Sí	Sí	Sí	Sí	Sí	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fránco t)	Europa (Londres)	Europa (París)	Europa (Estocolm o)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Backup::Resto reTestingPlan	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::BackupGateway ::Hypervisor	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::Batch::Comput eEnvironment	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Batch::JobQueue	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Batc h::SchedulingPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Perfil de AWS::Bedr ock::ApplicationInference	Sí	Sí	Sí	Sí	No	No	No	No
AWS::Bedrock::Guardrail	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Bedr ock::KnowledgeBase	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Bedrock::Prompt	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::BedrockAgentC ore::BrowserCustom	Sí	Sí	No	No	No	No	No	No
AWS::BedrockAgentC ore::CodeInterpret erPersonalizado	Sí	Sí	No	No	No	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::BedrockAgentCore::Runtime	Sí	Sí	No	No	No	No	No	No
AWS::Cassandra::Keyspace	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::CleanRoomsML::TrainingDataset	Sí	Sí	Sí	No	Sí	No	No	No
AWS::Cloud9::EnvironmentEC2	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::CloudFormation::GuardHook	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudFormation::LambdaHook	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudFormation::Stack	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::CloudFormation::StackSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudTrail::EventDataTienda	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudTrail::Trail	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudWatch::Alarm	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudWatch::MetricStream	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::CodeArtifact::Domain	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::CodeArtifact::Repository	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::CodeBuild::Project	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CodeBuild::ReportGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CodeDeploy::Application	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::CodeDeploy::DeploymentConfig	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::CodeDeploy::DeploymentGroup	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::CodeGuruProfiler::ProfilingGroup	Sí	Sí	Sí	No	Sí	No	No	No
AWS::CodeGuruReviewer::RepositoryAssociation	Sí	Sí	Sí	No	Sí	No	No	No
AWS::CodePipeline::Pipeline	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Cognito::IdentityPool	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Cognito::UserPool	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Cognito::UserPoolCliente	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Cognito::UserPoolGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Comprehend::Flywheel	Sí	Sí	Sí	No	No	No	No	No
AWS::Config::AggregationAuthorization	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Config::ConfigurationRecorder	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Config::ConformancePack	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Conformidad de AWS::Config::ConformancePack	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Config::ResourceCompliance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Config::StoredQuery	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Connect::Instance	No	Sí	Sí	No	No	No	No	No
AWS::Connect::PhoneNumber	No	Sí	Sí	No	No	No	No	No
AWS::Connect::QuickConnect	No	Sí	Sí	No	No	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Connect::Rule	No	Sí	Sí	No	No	No	No	No
AWS::Connect::SecurityProfile	No	Sí	Sí	No	No	No	No	No
AWS::Connect::User	No	Sí	Sí	No	No	No	No	No
AWS::CustomerProfiles::Domain	No	Sí	Sí	No	No	No	No	No
AWS::CustomerProfiles::ObjectType	No	Sí	Sí	No	No	No	No	No
AWS::DMS::Certificate	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::DMS::Endpoint	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::DMS::EventSubscription	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::DMS::MigrationProject	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DMS::ReplicationInstance	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::DMS::ReplicationSubnetGrupo	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::DMS::ReplicationTask	Sí	Sí	Sí	Sí	Sí	Sí	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::DataSync::Agent	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::LocationEFS	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::LocationFSxLustre	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::DataSync::LocationFSxVentanas	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::DataSync::LocationHDFS	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::LocationNFS	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::LocationObjectAlmacenamiento	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::LocationS3	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::LocationSMB	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::Task	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Deadline::Fleet	Sí	Sí	No	No	No	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Deadline::Monitor	Sí	Sí	No	No	No	No	No	No
AWS::Deadline::QueueFleetAsociación	Sí	Sí	No	No	No	No	No	No
AWS::Detective::Graph	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::DynamoDB::Table	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Capacity Reservation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::CarrierGateway	Sí	Sí	Sí	Sí	No	No	No	No
AWS::EC2::ClientVpnPunto final	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::EC2::ClientVpnTargetNetworkAssociation	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::EC2: :CustomerGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: DHCPOptions	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2: EC2 Flota	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2: :EIP	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS:EC2:: EIPAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::EgressOnlyInternetGateway	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::EC2::FlowLog	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Host	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2: :IPAM	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: IPAMPool	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2: IPAMPool Cir	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2: IPAMResource Descubrimiento	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: IPAMResource DiscoveryAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: IPAMScope	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Instance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Instance ConnectPunto final	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::EC2::InternetGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::LaunchTemplate	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::EC2::NatGateway	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::EC2::NetworkAcl	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::NetworkInsightsAccessScope	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::EC2::NetworkInsightsAnálisis	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::EC2::NetworkInsightsRuta	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::EC2::NetworkInterface	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::PrefixList	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::RouteTable	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::EC2::SecurityGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SecurityGroupVpcAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SnapshotBlockPublicAccess	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SpotFleet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Subnet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SubnetCidrBloquear	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SubnetNetworkAclAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SubnetRouteTableAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::TrafficMirrorFiltrar	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::TrafficMirrorSession	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::TrafficMirrorObjetivo	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::EC2::TransitGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::EC2::TransitGatewayAdjunto	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::TransitGatewayConnect	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::EC2::TransitGatewayMulticastDomain	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::TransitGatewayRouteTable	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS:EC2: :VPC	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCBlockPublicAccessExclusion	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCBlockPublicAccessOptions	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCEndpoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCEndpoint ConnectionNotification	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCEndpoint Servicio	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCGateway Adjunto	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCPeering Conexión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS:EC2:: VPNConnection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPNConnection Ruta	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPNGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Verified AccessInstancia	Sí	Sí	Sí	No	Sí	Sí	No	No
AWS::EC2::Volume	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::PullThroughCacheRule	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::RegistryPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::ReplicationConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::Repository	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::RepositoryCreationPlantilla	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS: :CapacityProvider	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::Cluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::ECS::Service	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::TaskDefinition	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::TaskSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EFS::AccessPoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EFS::FileSystem	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EKS::Addon	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EKS::Cluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EKS::FargateProfile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EKS::IdentityProviderConfig	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EMR::SecurityConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EMR::Studio	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EMRContainers::VirtualCluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::EMRServerless::Application	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::ElasticBeanstalk::Application	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ElasticBeanstalk::ApplicationVersion	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ElasticBeanstalk::Environment	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ElasticLoadBalancing::LoadBalancer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ElasticLoadBalancingV2::Listener	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::ElasticLoadBalancingV2::LoadBalancer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ElasticLoadBalancingV2::TargetGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Elasticsearch::Domain	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EntityResolution::IdMappingfluj o de trabajo	Sí	Sí	Sí	No	No	No	No	No
AWS::EntityResolution::MatchingWorkflow	Sí	Sí	Sí	No	No	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::EntityResolution::SchemaMapping	Sí	Sí	Sí	No	No	No	No	No
AWS::EventSchemas::Discoverer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EventSchemas::Registry	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EventSchemas::RegistryPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EventSchemas::Schema	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Events::ApiDestination	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Events::Archive	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Events::Connection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Events::Endpoint	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::Events::EventBus	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Events::Rule	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::FIS::ExperimentTemplate	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Forecast::Dataset	Sí	Sí	No	No	No	No	No	No
AWS::Forecast::DatasetGroup	Sí	Sí	No	No	No	No	No	No
AWS::FraudDetector::EntityType	Sí	No	No	No	No	No	No	No
AWS::FraudDetector::Label	Sí	No	No	No	No	No	No	No
AWS::FraudDetector::Outcome	Sí	No	No	No	No	No	No	No
AWS::FraudDetector::Variable	Sí	No	No	No	No	No	No	No
AWS::GameLift::Alias	Sí	Sí	Sí	No	No	No	No	No
AWS::GameLift::Build	Sí	Sí	Sí	No	No	No	No	No
AWS::GameLift::GameSessionCola	Sí	Sí	Sí	No	No	No	No	No
AWS::GameLift::MatchmakingConfiguration	Sí	Sí	No	No	No	No	No	No
AWS::Glue::Classifier	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Glue::Database	Sí	Sí	Sí	Sí	Sí	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Glue::Job	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Glue::MLTransform	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Glue::Registry	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::Grafana::Workspace	Sí	Sí	Sí	No	No	No	No	No
AWS::GreengrassV2::ComponentVersion	Sí	Sí	Sí	No	No	No	No	No
AWS::GroundStation::Config	Sí	Sí	No	No	Sí	No	No	No
AWS::GroundStation::DataflowEndpointGrupo	Sí	Sí	No	No	Sí	No	No	No
AWS::GroundStation::MissionProfile	Sí	Sí	No	No	Sí	No	No	No
AWS::GuardDuty::Detector	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::GuardDuty::Filter	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::GuardDeber: IPSet	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::GuardDuty::MalwareProtectionPlan	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::GuardDuty::ThreatIntelSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::HealthLago::FHIRDatastore	Sí	No	Sí	No	No	No	No	No
AWS::IAM::Group	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::IAM::Policy	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::IAM::Role	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::IAM::User	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::IVS::Channel	Sí	Sí	No	No	No	No	No	No
AWS::IVS::PlaybackKeyPareja	Sí	Sí	No	No	No	No	No	No
AWS::IVS::RecordingConfiguration	Sí	Sí	No	No	No	No	No	No
AWS::ImageBuilder::ContainerRecipe	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ImageBuilder::DistributionConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ImageBuilder::ImagePipeline	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::ImageBuilder::ImageRecipe	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ImageBuilder::InfrastructureConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ImageBuilder::LifecyclePolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::InspectorV2::Activation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::InspectorV2::Filter	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::IoT::AccountAuditConfiguración	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::Authorizer	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT:: CACertificate	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::CustomMetric	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::Dimension	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::DomainConfiguration	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::FleetMetric	Sí	Sí	Sí	Sí	Sí	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::IoT::JobTemplate	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::MitigationAction	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::Policy	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::ProvisioningTemplate	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::RoleAlias	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::ScheduledAudit	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::SecurityProfile	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::IoT::ThingGroup	Sí	Sí	Sí	Sí	Sí	No	Sí	No
AWS::IoTAnalytics::Channel	Sí	Sí	No	No	No	No	No	No
AWS::IoTAnalytics::Dataset	Sí	Sí	No	No	No	No	No	No
AWS::IoTAnalytics::Datastore	Sí	Sí	No	No	No	No	No	No
AWS::IoTAnalytics::Pipeline	Sí	Sí	No	No	No	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::IoTCoreDeviceAdvisor::SuiteDefinition	Sí	No	No	No	No	No	No	No
AWS::IoTEvents::AlarmModel	Sí	Sí	Sí	No	No	No	No	No
AWS::IoTEvents::DetectorModel	Sí	Sí	Sí	No	No	No	No	No
AWS::IoTEvents::Input	Sí	Sí	Sí	No	No	No	No	No
AWS::IoTSiteWise::Asset	Sí	Sí	No	No	No	No	No	No
AWS::IoTSiteWise::AssetModel	Sí	Sí	No	No	No	No	No	No
AWS::IoTSiteWise::Dashboard	Sí	Sí	No	No	No	No	No	No
AWS::IoTSiteWise::Gateway	Sí	Sí	No	No	No	No	No	No
AWS::IoTSiteWise::Portal	Sí	Sí	No	No	No	No	No	No
AWS::IoTSiteWise::Project	Sí	Sí	No	No	No	No	No	No
AWS::IoTTwinMaker::ComponentType	Sí	Sí	No	No	No	No	No	No
AWS::IoTTwinMaker::Entity	Sí	Sí	No	No	No	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::IoTTwinMaker::Scene	Sí	Sí	No	No	No	No	No	No
AWS::IoTTwinMaker::SyncJob	Sí	Sí	No	No	No	No	No	No
AWS::IoTTwinMaker::Workspace	Sí	Sí	No	No	No	No	No	No
AWS::IoTWireless::FuotaTask	Sí	Sí	No	No	No	No	No	No
AWS::IoTWireless::MulticastGroup	Sí	Sí	No	No	No	No	No	No
AWS::IoTWireless::ServiceProfile	Sí	Sí	No	No	No	No	No	No
AWS::KMS::Alias	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::KMS::Key	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::KafkaConnect::Connector	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::KafkaConnect::CustomPlugin	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::Kendra::Index	Sí	No	Sí	No	No	No	No	No
AWS::Kinesis::Stream	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Kinesis::StreamConsumer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::KinesisAnalyticsV2::Application	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::KinesisFirehose::DeliveryStream	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::KinesisVideo::SignalingChannel	Sí	Sí	Sí	Sí	No	No	No	No
AWS::KinesisVideo::Stream	Sí	Sí	Sí	Sí	No	No	No	No
AWS::Lambda::CodeSigningConfig	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::Lambda::Function	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Lex::Bot	Sí	Sí	Sí	No	No	No	No	No
AWS::Lex::BotAlias	Sí	Sí	Sí	No	No	No	No	No
AWS::Lightsail::Bucket	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::Lightsail::Certificate	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::Lightsail::Disk	Sí	Sí	Sí	Sí	Sí	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Lightsail::StaticIp	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::Location::APIKey	Sí	Sí	Sí	No	Sí	No	No	No
AWS::Location::GeofenceCollection	Sí	Sí	Sí	No	Sí	No	Sí	No
AWS::Location::Map	Sí	Sí	Sí	No	Sí	No	Sí	No
AWS::Location::PlaceIndex	Sí	Sí	Sí	No	Sí	No	Sí	No
AWS::Location::RouteCalculator	Sí	Sí	Sí	No	Sí	No	Sí	No
AWS::Logs::Destination	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::LookoutVision::Project	Sí	Sí	No	No	No	No	No	No
AWS::M2::Environment	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::MSK::BatchScramSecreto	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::MSK::Cluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::MSK::ClusterPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::MSK::Configuration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::MSK::ServerlessCluster	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MSK::VpcConnection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Macie::Session	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::MediaConnect::FlowEntitlement	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaConnect::FlowSource	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaConnect::FlowVpcInterfaz	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaConnect::Gateway	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaLive::Multiplexprogram	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaPackage::Asset	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaPackage::PackagingConfiguration	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaPackage::PackagingGroup	Sí	Sí	Sí	Sí	Sí	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::MediaPackageV2::Channel	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaPackageV2::ChannelGroup	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaPackageV2::OriginEndpoint	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::MediaTailor::LiveSource	Sí	Sí	No	Sí	Sí	No	No	No
AWS::MediaTailor::PlaybackConfiguration	Sí	Sí	No	Sí	Sí	No	No	No
AWS::MemoryDB::SubnetGroup	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::NetworkFirewall::Firewall	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::FirewallPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::RuleGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall: TLSInspection Configuración	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::VpcEndpointAsociación	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Omics::RunGroup	Sí	Sí	Sí	No	No	No	No	No
AWS::Omics::Workflow	Sí	Sí	Sí	No	No	No	No	No
AWS::Open Search::Domain	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::OpenSearchServerless::Collection	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::OpenSearchServerless::SecurityConfig	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::OpenSearchServerless::VpcEndpoint	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::PCAConnectorAD::Connector	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::PCAConnectorAD::DirectoryRegistration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Panorama::Package	Sí	No	No	No	No	No	No	No
AWS::Personalize::Dataset	Sí	Sí	No	No	No	No	No	No
AWS::Personalize:: DatasetGroup	Sí	Sí	No	No	No	No	No	No
AWS::Personalize::Schema	Sí	Sí	No	No	No	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Personalize::Solution	Sí	Sí	No	No	No	No	No	No
AWS::Pinpoint::App	Sí	Sí	Sí	No	No	No	No	No
AWS::Pinpoint::ApplicationSettings	Sí	Sí	Sí	No	No	No	No	No
AWS::Pinpoint::Campaign	Sí	Sí	Sí	No	No	No	No	No
AWS::Pinpoint::EmailChannel	Sí	Sí	Sí	No	No	No	No	No
AWS::Pinpoint::EmailTemplate	Sí	Sí	Sí	No	No	No	No	No
AWS::Pinpoint::EventStream	Sí	Sí	Sí	No	No	No	No	No
AWS::Pinpoint::InAppPlantilla	Sí	Sí	Sí	No	No	No	No	No
AWS::Pinpoint::Segment	Sí	Sí	Sí	No	No	No	No	No
AWS::QuickSight::Dashboard	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
AWS::QuickSight::DataSource	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::QuickSight::Template	Sí	Sí	Sí	Sí	Sí	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::QuickSight::Theme	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS: :RDS: DBCluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Instantánea DBCluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS: DBInstance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Punto final DBProxy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Grupo DBSecurity	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS: DBSnapshot	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Grupo DBSubnet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RDS: :EventSubscription	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RDS::GlobalCluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RDS::Integration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RDS::OptionGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::RUM::AppMonitor	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::Cluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterParameterGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSecurityGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSnapshot	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSubnetGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::EndpointAccess	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::Redshift::EndpointAuthorization	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::Redshift::EventSubscription	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::Integration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ScheduledAction	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::ResilienceHub::App	Sí	Sí	Sí	Sí	Sí	Sí	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::ResilienceHub::ResiliencyPolicy	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::ResourceExplorer2::Index	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RoboMaker::RobotApplication	Sí	Sí	No	No	No	No	No	No
AWS::RoboMaker::RobotApplicationVersión	Sí	Sí	No	No	No	No	No	No
AWS::RoboMaker::SimulationApplication	Sí	Sí	No	No	No	No	No	No
AWS::RolesEncualquier lugar: :CRL	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RolesAnywhere::Profile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RolesAnywhere::TrustAnchor	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Profiles::Profile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Profiles::ProfileAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Resolver::FirewallDomainLista	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::Route53Resolver::FirewallRuleGrupo	Sí	Sí	Sí	Sí	Sí	Sí	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverEndpoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
AWS::Route53Resolver::ResolverRule	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverRuleAsociación	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::AccessGrant	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::AccessGrantsInstancia	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::AccessGrantsLocation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::AccessPoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::AccountPublicAccessBlock	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::S3::Bucket	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::StorageLens	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::S3::StorageLensGrupo	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::S3Express::BucketPolicy	Sí	No	No	No	Sí	No	No	No
AWS::S3Express::DirectoryBucket	Sí	No	No	No	Sí	No	No	No
AWS::S3Tables::TableBucket	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3Tables::TableBucketPolítica	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SES::ConfigurationSet	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SES::ContactList	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SES::DedicatedIpPiscina	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SES::MailManagerTrafficPolicy	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::SES::ReceiptFilter	Sí	Sí	Sí	Sí	Sí	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::SES::ReceiptRuleSet	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::SES::Template	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SNS::Topic	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SQS::Queue	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SSM::AssociationCompliance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSM::Document	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSM::FileData	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Inventario de AWS::SSM::ManagedInstance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSM::PatchCompliance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSM::ResourceDataSincronizar	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSMContacts::Contact	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::SSMIncidents::ResponsePlan	Sí	Sí	Sí	Sí	Sí	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::SageMaker::AppImageConfig	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
AWS::SageMaker::CodeRepository	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SageMaker::DataQualityJobDefinition	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::SageMaker::Domain	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SageMaker::EndpointConfig	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SageMaker::FeatureGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
AWS::SageMaker::Image	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
AWS::SageMaker::InferenceExperiment	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SageMaker::MlflowTrackingServidor	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SageMaker::Model	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SageMaker::ModelBiasJobDefinition	Sí	Sí	Sí	Sí	Sí	No	No	No

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::SageMaker::ModelExplainabilityJobDefinition	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::SageMaker::ModelQualityJobDefinition	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::SageMaker::MonitoringSchedule	Sí	Sí	Sí	Sí	Sí	No	No	No
AWS::SageMaker::NotebookInstance	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::SageMaker::StudioLifecycleConfig	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SageMaker::UserProfile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SageMaker::Workteam	Sí	Sí	Sí	No	No	No	No	No
AWS::SecretsManager::ResourcePolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SecretsManager::RotationSchedule	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SecretsManager::Secret	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fránco t)	Europa (Londres)	Europa (París)	Europa (Estocolm o)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::Secu rityHub::Standard	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ServiceCatalo g::CloudFormationProducto	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ServiceCatalo g::CloudFormationP rovisionedProduct	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Serv iceCatalog::Portfolio	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ServiceDiscov ery::HttpNamespace	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ServiceDiscov ery::Instance	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::ServiceDiscov ery::PublicDnsEspa cio de nombres	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ServiceDiscov ery::Service	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::ShieldRegiona l::Protection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Sign er::SigningProfile	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::Step Functions::Activity	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fráncfort)	Europa (Londres)	Europa (París)	Europa (Estocolmo)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::StepFunctions::StateMachine	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Transfer::Agreement	Sí	Sí	Sí	Sí	Sí	Sí	No	No
AWS::Transfer::Certificate	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Transfer::Connector	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Transfer::Profile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Transfer::Server	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Transfer::Workflow	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFRegional::RateBasedRegla	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFRegional::Rule	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFRegional::RuleGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFRegional::WebACL	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:WAFv2:: IPSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Europa (Irlanda)	Europa (Fránco t)	Europa (Londres)	Europa (París)	Europa (Estocolm o)	Europa (Milán)	Europa (España)	Europa (Zúrich)
AWS::WAFv 2::ManagedRuleSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv 2::RegexPatternSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv2::RuleGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv2::WebACL	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WorkSpaces::C onnectionAlias	Sí	Sí	Sí	No	No	No	No	No
AWS::Work Spaces::Workspace	Sí	Sí	Sí	No	No	No	No	No
AWS::XRay ::EncryptionConfig	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Regiones de Asia-Pacífico

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapo)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::ACM: :Certificate	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::ACMPCA::CertificateAuthority	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ACMPCA::CertificateAuthorityActivación	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::APS::RuleGroupsEspacio de nombres	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::AccessAnalyzer::Analyzer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AmazonMQ::Broker	Sí	No	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Amplify::App	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Amplify::Branch	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ApiGateway::DomainName	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGateway::Method	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::ApiGateway::RestApi	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ApiGateway::Stage	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ApiGateway::UsagePlan	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Api	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ApiGatewayV2::Integration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ApiGatewayV2::Stage	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::AppConfig::Application	Sí	No	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppConfig::ConfigurationProfile	Sí	No	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppConfig::DeploymentStrategy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::AppConfig::Environment	Sí	No	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppConfig::Extension	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::AppConfig::ExtensionAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppConfig::HostedConfigurationVersión	Sí	No	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppFlow::Flow	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::AppIntegrations::Application	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::AppIntegrations::DataIntegration	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::AppIntegrations::EventIntegration	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::AppMesh::GatewayRoute	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppMesh::Mesh	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppMesh::Route	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppMesh::VirtualGateway	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppMesh::VirtualNode	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppMesh::VirtualRouter	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppMesh::VirtualService	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AppRunner::Service	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::AppRunner::VpcConnector	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::AppStream::AppBlockConstructor	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::AppStream::Application	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::AppStream::DirectoryConfig	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::AppStream::Fleet	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::AppStream::Stack	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::AppSync::Api	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::AppSync::ApiCache	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::AppSync::GraphQLApi	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Athena::DataCatalog	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Athena::PreparedStatement	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Athena::WorkGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::AuditManager::Assessment	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::AutoScaling::AutoScalingGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::LaunchConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::ScalingPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::ScheduledAction	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::AutoScaling::WarmPool	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Backup::BackupPlan	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Backup::BackupSelection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Backup::BackupVault	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Backup::RecoveryPoint	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Backup::ReportPlan	Sí	Sí	Sí	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Backup::RestoreTestingPlanificar	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::BackupGateway::Hypervisor	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Batch::ComputeEnvironment	Sí	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Batch::JobQueue	Sí	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Batch::SchedulingPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
Perfil de AWS::Bedrock::ApplicationInference	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Bedrock::Guardrail	No	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Bedrock::KnowledgeBase	No	Sí	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Bedrock::Prompt	No	Sí	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::BedrockAgentCore::BrowserCustom	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::BedrockAgentCore::CodeInterpreterPersonalizado	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::BedrockAgentCore::Runtime	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::Cassandra::Keyspace	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::CleanRoomsML::TrainingDataset	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::Cloud9::EnvironmentEC2	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CloudFormation::GuardHook	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CloudFormation::LambdaHook	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CloudFormation::Stack	Sí	No	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudFormation::StackSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::CloudTrail::EventDataTienda	Sí	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CloudTrail::Trail	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::CloudWatch::Alarm	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::CloudWatch::MetricStream	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CodeArtifact::Domain	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::CodeArtifact::Repository	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::CodeBuild::Project	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CodeBuild::ReportGroup	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CodeDeploy::Application	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CodeDeploy::DeploymentConfig	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CodeDeploy::DeploymentGroup	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::CodeGuruProfiler::ProfilingGroup	No	No	No	No	No	No	No	No	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::CodeGuruReviewer::RepositoryAssociation	No	No	No	No	No	No	No	No	Sí	Sí	No	No	Sí
AWS::CodePipeline::Pipeline	Sí	Sí	No	No	Sí	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Cognito::IdentityPool	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Cognito::UserPool	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Cognito::UserPoolCliente	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Cognito::UserPoolGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Comprehend::Flywheel	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Config::AggregationAuthorization	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Config::ConfigurationRecorder	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Config::ConformancePack	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
Conformidad de AWS::Config::ConformancePack	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Config::ResourceCompliance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Config::StoredQuery	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Connect::Instance	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::Connect::PhoneNumber	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::Connect::QuickConnect	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::Connect::Rule	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::Connect::SecurityProfile	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Connect::User	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::CustomerProfiles::Domain	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::CustomerProfiles::ObjectType	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::DMS::Certificate	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DMS::Endpoint	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DMS::EventSubscription	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DMS::MigrationProject	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DMS::ReplicationInstance	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DMS::ReplicationSubnetGrupo	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::DMS::ReplicationTask	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DataSync::Agent	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::DataSync::LocationEFS	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DataSync::LocationFSxLustre	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DataSync::LocationFSxWindows	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DataSync::LocationHDFS	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DataSync::LocationNFS	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DataSync::LocationObjectAlmacenamiento	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DataSync::LocationS3	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::DataSync::LocationSMB	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::DataSync::Task	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Deadline::Fleet	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::Deadline::Monitor	No	No	No	No	No	No	No	No	Sí	Sí	No	No	Sí
AWS::Deadline::QueueFleetAsociación	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::Detective::Graph	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::DynamoDB::Table	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::CapacityReservation	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::CarrierGateway	No	No	No	No	No	No	No	Sí	No	Sí	No	No	Sí
AWS::EC2::ClientVpnPunto final	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::EC2::ClientVpnTargetNetworkAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::Customer Gateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2::DHCPOptions	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2: EC2 Flota	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS:EC2: :EIP	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2::EIPAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::EgressOnlyInternetGateway	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::FlowLog	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::Host	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2: :IPAM	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS:EC2::IPAMPool	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS:EC2:IPAMPool Cir	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2:IPAMResource Descubrimiento	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS:EC2::IPAMResource Discovery Association	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS:EC2::IPAMScope	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::Instance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Instance ConnectPunto final	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::InternetGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::LaunchTemplate	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::EC2::NatGateway	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::NetworkAcl	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::NetworkInsightsAccessScope	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::NetworkInsightsAnálisis	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::EC2::NetworkInsightsRuta	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::NetworkInterface	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::PrefixList	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::RouteTable	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::EC2::SecurityGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SecurityGroupVpcAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SnapshotBlockPublicAccess	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::SpotFleet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::Subnet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SubnetCidrBloquear	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::SubnetNetworkAclAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::SubnetRouteTableAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::EC2::TrafficMirrorFiltro	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::TrafficMirrorSession	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::TrafficMirrorObjetivo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::TransitGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::TransitGatewayAdjunto	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EC2::TransitGatewayConnect	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::TransitGatewayMulticastDomain	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EC2::TransitGatewayRouteTable	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS:EC2: :VPC	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCBlock PublicAccessExclusion	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS:EC2:: VPCBlock PublicAccessOptions	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS:EC2:: VPCEndpoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCEndpoint ConnectionNotification	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS:EC2:: VPCEndpoint Servicio	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCGateway Adjunto	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2:: VPCPeering Conexión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS:EC2::VPNConnection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS:EC2::VPNConnection Ruta	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS:EC2::VPNGateway	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EC2::Verified AccessInstancia	No	No	Sí	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::EC2::Volume	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::PullThroughCacheRule	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ECR::RegistryPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ECR::ReplicationConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECR::Repository	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::ECR::RepositoryCreationPlantilla	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::CapacityProvider	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ECS::Cluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::Service	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::TaskDefinition	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ECS::TaskSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EFS::AccessPoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EFS::FileSystem	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::EKS::Addon	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EKS::Cluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EKS::FargateProfile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::EKS::IdentityProviderConfig	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EMR::SecurityConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EMR::Studio	Sí	No	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EMRContainers::VirtualCluster	Sí	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EMRServerless::Application	Sí	Sí	Sí	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::ElasticBeanstalk::Application	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ElasticBeanstalk::ApplicationVersion	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ElasticBeanstalk::Environment	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::ElasticLoadBalancing::LoadBalancer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ElasticLoadBalancingV2::Listener	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ElasticLoadBalancingV2::LoadBalancer	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::ElasticLoadBalancingV2::TargetGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Elasticsearch::Domain	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::EntityResolution::IdMappingflujo de trabajo	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::EntityResolution::MatchingWorkflow	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::EntityResolution::SchemaMapping	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::EventSchemas::Discoverer	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EventSchemas::Registry	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EventSchemas::RegistryPolicy	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::EventSchemas::Schema	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Events::ApiDestination	Sí	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Events::Archive	Sí	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Events::Connection	Sí	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Events::Endpoint	No	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Events::EventBus	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Events::Rule	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::FIS::ExperimentTemplate	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Forecast::Dataset	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Forecast::DatasetGroup	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::FraudDetector::EntityType	No	No	No	No	No	No	No	No	Sí	Sí	No	No	No
AWS::FraudDetector::Label	No	No	No	No	No	No	No	No	Sí	Sí	No	No	No
AWS::FraudDetector::Outcome	No	No	No	No	No	No	No	No	Sí	Sí	No	No	No
AWS::FraudDetector::Variable	No	No	No	No	No	No	No	No	Sí	Sí	No	No	No

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::GameLift::Alias	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::GameLift::Build	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::GameLift::GameSessionQueue	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::GameLift::MatchmakingConfiguration	No	No	No	No	No	No	No	Sí	No	Sí	No	No	Sí
AWS::Glue::Classifier	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Glue::Database	Sí	Sí	Sí	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Glue::Job	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Glue::MLTransform	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Glue::Registry	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Grafana::Workspace	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::GreengrassV2::ComponentVersion	No	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::GroundStation::Config	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	No
AWS::GroundStation::DataflowEndpointGrupo	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	No
AWS::GroundStation::MissionProfile	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	No
AWS::GuardDuty::Detector	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::GuardDuty::Filter	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::GuardDeber: IPSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::GuardDuty::MalwareProtectionPlan	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::GuardDuty::ThreatIntelSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::HealthLago:FHIRDatastore	No	No	No	No	No	Sí	No	No	No	No	No	No	No
AWS::IAM::Group	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::IAM::Policy	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::IAM::Role	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::IAM::User	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::IVS::Channel	No	No	No	No	No	Sí	No	Sí	No	No	No	No	Sí
AWS::IVS::PlaybackKeyPareja	No	No	No	No	No	Sí	No	Sí	No	No	No	No	Sí
AWS::IVS::RecordingConfiguration	No	No	No	No	No	Sí	No	Sí	No	No	No	No	Sí
AWS::ImageBuilder::ContainerRecipe	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ImageBuilder::DistributionConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::ImageBuilder::ImagePipeline	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ImageBuilder::ImageRecipe	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ImageBuilder::InfrastructureConfiguration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ImageBuilder::LifecyclePolicy	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::InspectorV2::Activation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::InspectorV2::Filter	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::IoT::AccountAuditConfiguración	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::Authorizer	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::CACertificate	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::IoT::CustomMetric	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::Dimension	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::DomainConfiguration	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::FleetMetric	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::JobTemplate	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::MitigationAction	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::Policy	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::ProvisioningTemplate	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::RoleAlias	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::ScheduledAudit	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::IoT::SecurityProfile	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoT::ThingGroup	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTAnalytics::Channel	No	No	No	No	No	Sí	No	No	No	Sí	No	No	Sí
AWS::IoTAnalytics::Dataset	No	No	No	No	No	Sí	No	No	No	Sí	No	No	Sí
AWS::IoTAnalytics::Datastore	No	No	No	No	No	Sí	No	No	No	Sí	No	No	Sí
AWS::IoTAnalytics::Pipeline	No	No	No	No	No	Sí	No	No	No	Sí	No	No	Sí
AWS::IoTCoreDeviceAdvisor::SuiteDefinition	No	No	No	No	No	No	No	No	No	No	No	No	Sí
AWS::IoTEvents::AlarmModel	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTEvents::DetectorModel	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTEvents::Input	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::IoTSiteWise::Asset	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTSiteWise::AssetModel	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTSiteWise::Dashboard	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTSiteWise::Gateway	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTSiteWise::Portal	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTSiteWise::Project	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTTwinMaker::ComponentType	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTTwinMaker::Entity	No	No	No	No	No	No	No	No	Sí	Sí	No	No	No
AWS::IoTTwinMaker::Scene	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTTwinMaker::SyncJob	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::IoTTwinMaker::Workspace	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::IoTWireless::FuotaTask	No	No	No	No	No	No	No	No	No	Sí	No	No	Sí
AWS::IoTWireless::MulticastGroup	No	No	No	No	No	No	No	No	No	Sí	No	No	Sí
AWS::IoTWireless::ServiceProfile	No	No	No	No	No	No	No	No	No	Sí	No	No	Sí
AWS::KMS::Alias	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::KMS::Key	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::KafkaConnect::Connector	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::KafkaConnect::CustomPlugin	Sí	Sí	Sí	Sí	No	Sí	No	Sí	Sí	Sí	No	Sí	Sí
AWS::Kendra::Index	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Kinesis::Stream	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Kinesis::StreamConsumer	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::KinesisAnalyticsV2::Application	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::KinesisFirehose::DeliveryStream	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::KinesisVideo::SignalingChannel	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::KinesisVideo::Stream	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Lambda::CodeSigningConfig	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Lambda::Function	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Lex::Bot	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Lex::BotAlias	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::Lightsail::Bucket	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Lightsail::Certificate	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Lightsail::Disk	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Lightsail::StaticIp	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Location::APIKey	No	No	No	No	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::Location::GeofenceCollection	No	No	No	Sí	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::Location::Map	No	No	No	Sí	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::Location::PlaceIndex	No	No	No	Sí	No	Sí	No	No	Sí	Sí	No	No	Sí
AWS::Location::RouteCalculator	No	No	No	Sí	No	Sí	No	No	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Logs::Destination	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::LookoutVision::Project	No	No	No	No	No	No	No	Sí	No	No	No	No	Sí
AWS::M2::Environment	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::MSK::BatchScramSecreto	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MSK::Cluster	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MSK::ClusterPolicy	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MSK::Configuration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MSK::ServerlessCluster	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::MSK::VpcConnection	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Macie::Session	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::MediaConnect::FlowEntitlement	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaConnect::FlowSource	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaConnect::FlowVpcInterfaz	Sí	Sí	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaConnect::Gateway	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaLive::Multiplexprogram	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaPackage::Asset	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaPackage::PackagingConfiguration	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaPackage::PackagingGroup	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::MediaPackageV2::Channel	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaPackageV2::ChannelGroup	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaPackageV2::OriginEndpoint	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaTailor::LiveSource	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MediaTailor::PlaybackConfiguration	No	No	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::MemoryDB::SubnetGroup	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::NetworkFirewall::Firewall	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::FirewallPolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::NetworkFirewall::RuleGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::TLSInspectionConfiguración	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::VpcEndpointAsociación	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Omics::RunGroup	No	No	No	No	No	No	No	Sí	Sí	No	No	No	No
AWS::Omics::Workflow	No	No	No	No	No	No	No	Sí	Sí	No	No	No	No
AWS::OpenSearch::Domain	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::OpenSearchServerless::Collection	Sí	Sí	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::OpenSearchServerless::SecurityConfig	Sí	Sí	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::OpenSearchServerless::VpcEndpoint	Sí	Sí	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::PCAConnectorAD::Connector	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::PCAConnectorAD::DirectoryRegistration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Panorama::Package	No	No	No	No	No	No	No	No	Sí	Sí	No	No	No
AWS::Personalize::Dataset	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Personalize::DatasetGroup	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Personalize::Schema	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Personalize::Solution	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Pinpoint::App	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Pinpoint::ApplicationSettings	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Pinpoint::Campaign	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Pinpoint::EmailChannel	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Pinpoint::EmailTemplate	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Pinpoint::EventStream	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Pinpoint::InAppPlantilla	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Pinpoint::Segment	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::QuickSight::Dashboard	No	No	Sí	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::QuickSight::DataSource	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::QuickSight::Template	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::QuickSight::Theme	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS: :RDS: DBCluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Instantánea DBCluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS: DBInstance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Punto final DBProxy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS: :RDS:: Grupo DBSecurity	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS: DBSnapshot	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS: :RDS:: Grupo DBSubnet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RDS: :EventSubscription	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::RDS::GlobalCluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::RDS::Integration	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::RDS::OptionGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::RUM::AppMonitor	No	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Redshift::Cluster	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterParameterGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSecurityGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSnapshot	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSubnetGrupo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Redshift::EndpointAccess	Sí	Sí	Sí	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Redshift::EndpointAuthorization	Sí	Sí	Sí	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::Redshift::EventSubscription	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Redshift::Integration	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Redshift::ScheduledAction	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::ResilienceHub::App	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::ResilienceHub::ResiliencyPolicy	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::ResourceExplorer2::Index	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::RoboMaker::RobotApplication	No	No	No	No	No	No	No	No	Sí	No	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::RoboMaker::RobotApplicationVersión	No	No	No	No	No	No	No	No	Sí	No	No	No	Sí
AWS::RoboMaker::SimulationApplication	No	No	No	No	No	No	No	No	Sí	No	No	No	Sí
AWS::RolesEn cualquier lugar: :CRL	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::RolesAnywhere::Profile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::RolesAnywhere::TrustAnchor	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Profiles::Profile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Route53Profiles::ProfileAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Route53Resolver::FirewallDomainLista	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Route53Resolver::FirewallRuleGrupo	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Route53Resolver::ResolverEndpoint	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Route53Resolver::ResolverRule	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Route53Resolver::ResolverRuleAsociación	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::S3::AccessGrant	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::S3::AccessGrantsInstancia	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::S3::AccessGrantsLocation	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::S3::AccessPoint	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::S3::AccountPublicAccessBlock	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::S3::Bucket	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::S3::StorageLens	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::S3::StorageLensGrupo	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::S3Express::BucketPolicy	No	No	No	No	No	Sí	No	No	No	No	No	No	Sí
AWS::S3Express::DirectoryBucket	No	No	No	No	No	Sí	No	No	No	No	No	No	Sí
AWS::S3Tables::TableBucket	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::S3Tables::TableBucketPolítica	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::SES::ConfigurationSet	No	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SES::ContactList	No	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SES::DedicatedIpPiscina	No	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SES::MailManagerTrafficPolicy	No	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::SES::ReceiptFilter	No	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SES::ReceiptRuleSet	No	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SES::Template	No	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SNS::Topic	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SQS::Queue	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SSM::AssociationCompliance	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSM::Document	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SSM::FileData	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí
Inventario de AWS::SSM::ManagedInstance	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSM::PatchCompliance	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::SSM::ResourceDataSincronizar	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SSMContacts::Contact	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::SSMIncidents::ResponsePlan	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::AppImageConfig	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::CodeRepository	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::DataQualityJobDefinition	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::Domain	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::EndpointConfig	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::SageMaker::FeatureGroup	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::Image	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::InferenceExperiment	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::MlflowTrackingServidor	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SageMaker::Model	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::ModelBiasJobDefinition	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::ModelExplainabilityJobDefinition	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::SageMaker::ModelQualityJobDefinition	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::MonitoringSchedule	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::NotebookInstance	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sí	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::StudioLifecycleConfig	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::UserProfile	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::SageMaker::Workteam	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::SecretsManager::ResourcePolicy	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SecretsManager::RotationSchedule	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SecretsManager::Secret	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::SecurityHub::Standard	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::ServiceCatalog::CloudFormationProducto	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ServiceCatalog::Portfolio	Sí	Sí	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::ServiceDiscovery::HttpNamespace	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ServiceDiscovery::Instance	Sí	No	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ServiceDiscovery::PublicDnsEspacio de nombres	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::ServiceDiscovery::Service	Sí	No	No	Sí	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::ShieldRegional::Protection	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
AWS::Signer::SigningProfile	Sí	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::StepFunctions::Activity	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::StepFunctions::StateMachine	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Transfer::Agreement	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	No	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::Transfer::Certificate	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Transfer::Connector	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Transfer::Profile	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Transfer::Server	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::Transfer::Workflow	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::WAFRegional::RateBasedRegla	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::WAFRegional::Rule	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::WAFRegional::RuleGroup	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS::WAFRegional::WebACL	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	No	No	Sí
AWS:WAFv2 :: IPSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tipo de recurso	Asia-Pacífico (Hong Kong)	Asia-Pacífico (Hyderabad)	Asia-Pacífico (Yakarta)	Asia-Pacífico (Malasia)	Asia-Pacífico (Melbourne)	Asia-Pacífico (Mumbai)	Asia-Pacífico (Osaka)	Asia Pacífico (Seúl)	Asia-Pacífico (Singapur)	Asia Pacífico (Sídney)	Asia Pacífico (Taipéi)	Asia Pacífico (Tailandia)	Asia Pacífico (Tokio)
AWS::WAFv2::ManagedRuleSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv2::RegexPatternSet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv2::RuleGroup	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WAFv2::WebACL	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
AWS::WorkSpaces::ConnectionAlias	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No	Sí
AWS::WorkSpaces::Workspace	No	No	No	No	No	Sí	No	Sí	Sí	Sí	No	No	Sí
AWS::XRay::EncryptionConfig	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Regiones de China

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::ACM::Certificate	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::AmazonMQ::Broker	Sí	Sí
AWS::ApiGateway::DomainName	Sí	Sí
AWS::ApiGateway::Method	Sí	Sí
AWS::ApiGateway::RestApi	Sí	Sí
AWS::ApiGateway::Stage	Sí	Sí
AWS::ApiGateway::UsagePlan	Sí	Sí
AWS::ApiGatewayV2::Api	Sí	Sí
AWS::ApiGatewayV2::Integration	Sí	Sí
AWS::ApiGatewayV2::Stage	Sí	Sí
AWS::AppConfig::Application	Sí	Sí
AWS::AppConfig::ConfigurationProfile	Sí	Sí
AWS::AppConfig::DeploymentStrategy	Sí	Sí
AWS::AppConfig::Environment	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::AppConfig::Extension	Sí	Sí
AWS::AppConfig::ExtensionAssociation	Sí	Sí
AWS::AppConfig::HostedConfigurationVersión	Sí	Sí
AWS::AppSync::Api	Sí	Sí
AWS::AppSync::ApiCache	Sí	Sí
AWS::AppSync::GraphQLApi	Sí	Sí
AWS::Athena::DataCatalog	Sí	Sí
AWS::Athena::PreparedStatement	Sí	Sí
AWS::Athena::WorkGroup	Sí	Sí
AWS::AutoScaling::AutoScalingGrupo	Sí	Sí
AWS::AutoScaling::LaunchConfiguration	Sí	Sí
AWS::AutoScaling::ScalingPolicy	Sí	Sí
AWS::AutoScaling::ScheduledAction	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::AutoScaling::WarmPool	Sí	Sí
AWS::Backup::BackupPlan	Sí	Sí
AWS::Backup::BackupSelection	Sí	Sí
AWS::Backup::BackupVault	Sí	Sí
AWS::Backup::RecoveryPoint	Sí	Sí
AWS::Batch::ComputeEnvironment	Sí	Sí
AWS::Batch::JobQueue	Sí	Sí
AWS::Batch::SchedulingPolicy	Sí	Sí
AWS::Cassandra::Keyspace	Sí	Sí
AWS::CloudFormation::Stack	Sí	Sí
AWS::CloudFormation::StackSet	Sí	Sí
AWS::CloudFront::PublicKey	Sí	No
AWS::CloudTrail::Trail	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::CloudWatch::Alarm	Sí	Sí
AWS::CloudWatch::MetricStream	Sí	Sí
AWS::CodeBuild::Project	Sí	Sí
AWS::CodeBuild::ReportGroup	Sí	Sí
AWS::Cognito::IdentityPool	Sí	No
AWS::Config::AggregationAuthorization	Sí	Sí
AWS::Config::ConfigurationRecorder	Sí	Sí
AWS::Config::ResourceCompliance	Sí	Sí
AWS::Config::StoredQuery	Sí	Sí
AWS::DMS::Certificate	Sí	Sí
AWS::DMS::Endpoint	Sí	Sí
AWS::DMS::EventSubscription	Sí	Sí
AWS::DMS::ReplicationInstance	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::DMS::ReplicationSubnetGrupo	Sí	Sí
AWS::DMS::ReplicationTask	Sí	Sí
AWS::DataSync::Agent	Sí	Sí
AWS::DataSync::LocationEFS	Sí	Sí
AWS::DataSync::LocationHDFS	Sí	Sí
AWS::DataSync::LocationNFS	Sí	Sí
AWS::DataSync::LocationObjectAlmacenamiento	Sí	Sí
AWS::DataSync::LocationS3	Sí	Sí
AWS::DataSync::LocationSMB	Sí	Sí
AWS::DataSync::Task	Sí	Sí
AWS::DynamoDB::Table	Sí	Sí
AWS::EC2::CapacityReservation	Sí	Sí
AWS:EC2:: DHCPOptions	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::EC2: EC2 Flota	Sí	Sí
AWS:EC2: :EIP	Sí	Sí
AWS:EC2:: EIPAssociation	Sí	Sí
AWS::EC2::FlowLog	Sí	Sí
AWS::EC2::Host	Sí	Sí
AWS::EC2::Instance	Sí	Sí
AWS::EC2::InternetGateway	Sí	Sí
AWS::EC2::LaunchTemplate	Sí	Sí
AWS::EC2::NatGateway	Sí	Sí
AWS::EC2::NetworkAcl	Sí	Sí
AWS::EC2::NetworkInterface	Sí	Sí
AWS::EC2::PrefixList	Sí	Sí
AWS::EC2::RouteTable	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::EC2::SecurityGroup	Sí	Sí
AWS::EC2::SecurityGroupVpcAssociation	Sí	Sí
AWS::EC2::SnapshotBlockPublicAccess	Sí	Sí
AWS::EC2::SpotFleet	Sí	Sí
AWS::EC2::Subnet	Sí	Sí
AWS::EC2::SubnetCidrBloquear	Sí	No
AWS::EC2::SubnetNetworkAclAssociation	Sí	Sí
AWS::EC2::SubnetRouteTableAssociation	Sí	Sí
AWS::EC2::TrafficMirrorFiltro	Sí	Sí
AWS::EC2::TrafficMirrorSession	Sí	Sí
AWS::EC2::TrafficMirrorObjetivo	Sí	Sí
AWS::EC2::TransitGateway	Sí	Sí
AWS::EC2::TransitGatewayAdjunto	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::EC2::TransitGatewayConnect	Sí	Sí
AWS::EC2::TransitGatewayMulticastDomain	Sí	Sí
AWS::EC2::TransitGatewayRouteTable	Sí	Sí
AWS:EC2: :VPC	Sí	Sí
AWS:EC2:: VPCBlock PublicAccessExclusion	Sí	Sí
AWS:EC2:: VPCBlock PublicAccessOptions	Sí	Sí
AWS:EC2:: VPCEndpoint	Sí	Sí
AWS:EC2:: VPCEndpoint ConnectionNotification	Sí	Sí
AWS:EC2:: VPCEndpoint Servicio	Sí	Sí
AWS:EC2:: VPCGateway Adjunto	Sí	Sí
AWS:EC2:: VPCPeering Conexión	Sí	Sí
AWS:EC2:: VPNGateway	Sí	No
AWS::EC2::Volume	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::ECR::ReplicationConfiguration	Sí	Sí
AWS::ECR::Repository	Sí	Sí
AWS::ECS::CapacityProvider	Sí	Sí
AWS::ECS::Cluster	Sí	Sí
AWS::ECS::Service	Sí	Sí
AWS::ECS::TaskDefinition	Sí	Sí
AWS::ECS::TaskSet	Sí	Sí
AWS::EFS::AccessPoint	Sí	Sí
AWS::EFS::FileSystem	Sí	Sí
AWS::EKS::Addon	Sí	Sí
AWS::EKS::Cluster	Sí	Sí
AWS::EKS::FargateProfile	Sí	Sí
AWS::EKS::IdentityProviderConfig	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::EMR::SecurityConfiguration	Sí	Sí
AWS::EMR::Studio	Sí	Sí
AWS::EMRContainers::VirtualCluster	Sí	Sí
AWS::EMRServerless::Application	Sí	Sí
AWS::ElasticBeanstalk::Application	Sí	Sí
AWS::ElasticBeanstalk::ApplicationVersion	Sí	Sí
AWS::ElasticBeanstalk::Environment	Sí	Sí
AWS::ElasticLoadBalancing::LoadBalancer	Sí	Sí
AWS::ElasticLoadBalancingV2::Listener	Sí	Sí
AWS::ElasticLoadBalancingV2::LoadBalancer	Sí	Sí
AWS::ElasticLoadBalancingV2::TargetGroup	Sí	Sí
AWS::Elasticsearch::Domain	Sí	Sí
AWS::Events::Archive	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::Events::EventBus	Sí	Sí
AWS::Events::Rule	Sí	Sí
AWS::GameLift::Alias	Sí	Sí
AWS::GameLift::GameSessionCola	Sí	Sí
AWS::GameLift::MatchmakingConfiguration	Sí	Sí
AWS::Glue::Classifier	Sí	Sí
AWS::Glue::Job	Sí	Sí
AWS::Glue::MLTransform	Sí	No
AWS::Glue::Registry	Sí	Sí
AWS::GreengrassV2::ComponentVersion	Sí	No
AWS::GuardDuty::Filter	Sí	Sí
AWS::GuardDuty::ThreatIntelSet	Sí	Sí
AWS::IAM::Group	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::IAM::InstanceProfile	Sí	No
AWS: :IAM:: OIDCProvider	Sí	No
AWS::IAM::Policy	Sí	Sí
AWS::IAM::Role	Sí	Sí
AWS: :IAM:: SAMLProvider	Sí	No
AWS::IAM::ServerCertificate	Sí	No
AWS::IAM::User	Sí	Sí
AWS::ImageBuilder::ContainerRecipe	Sí	Sí
AWS::ImageBuilder::DistributionConfiguration	Sí	Sí
AWS::ImageBuilder::ImagePipeline	Sí	Sí
AWS::ImageBuilder::ImageRecipe	Sí	Sí
AWS::ImageBuilder::InfrastructureConfiguration	Sí	Sí
AWS::InspectorV2::Activation	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::IoT::AccountAuditConfiguración	Sí	Sí
AWS::IoT::Authorizer	Sí	Sí
AWS::IoT:: CACertificate	Sí	Sí
AWS::IoT::CustomMetric	Sí	Sí
AWS::IoT::Dimension	Sí	Sí
AWS::IoT::DomainConfiguration	Sí	Sí
AWS::IoT::FleetMetric	Sí	Sí
AWS::IoT::JobTemplate	Sí	Sí
AWS::IoT::MitigationAction	Sí	Sí
AWS::IoT::Policy	Sí	Sí
AWS::IoT::ProvisioningTemplate	Sí	Sí
AWS::IoT::RoleAlias	Sí	Sí
AWS::IoT::ScheduledAudit	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::IoT::SecurityProfile	Sí	Sí
AWS::IoT::ThingGroup	Sí	Sí
AWS::IoTAnalytics::Channel	Sí	No
AWS::IoTAnalytics::Dataset	Sí	No
AWS::IoTAnalytics::Datastore	Sí	No
AWS::IoTAnalytics::Pipeline	Sí	No
AWS::IoTEvents::AlarmModel	Sí	No
AWS::IoTEvents::DetectorModel	Sí	No
AWS::IoTEvents::Input	Sí	No
AWS::IoTSiteWise::Asset	Sí	No
AWS::IoTSiteWise::AssetModel	Sí	No
AWS::IoTSiteWise::Dashboard	Sí	No
AWS::IoTSiteWise::Gateway	Sí	No

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::IoTSiteWise::Portal	Sí	No
AWS::IoTSiteWise::Project	Sí	No
AWS::KMS::Alias	Sí	Sí
AWS::KMS::Key	Sí	Sí
AWS::Kinesis::Stream	Sí	Sí
AWS::Kinesis::StreamConsumer	Sí	Sí
AWS::KinesisAnalyticsV2::Application	Sí	Sí
AWS::KinesisFirehose::DeliveryStream	Sí	Sí
AWS::Lambda::Function	Sí	No
AWS::Logs::Destination	Sí	Sí
AWS::MSK::BatchScramSecreto	Sí	Sí
AWS::MSK::Cluster	Sí	Sí
AWS::MSK::ClusterPolicy	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::MSK::Configuration	Sí	Sí
AWS::MSK::VpcConnection	Sí	Sí
AWS::NetworkFirewall::Firewall	Sí	Sí
AWS::NetworkFirewall::FirewallPolicy	Sí	Sí
AWS::NetworkFirewall::RuleGroup	Sí	Sí
AWS::NetworkFirewall: TLSInspection Configuración	Sí	Sí
AWS::NetworkFirewall::VpcEndpointAsociación	Sí	Sí
AWS::OpenSearch::Domain	Sí	Sí
AWS::Personalize::Dataset	Sí	No
AWS::Personalize::DatasetGroup	Sí	No
AWS::Personalize::Schema	Sí	No
AWS::Personalize::Solution	Sí	No
AWS::QuickSight::Dashboard	Sí	No

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS: :RDS: DBCluster	No	Sí
AWS: :RDS:: Instantánea DBCluster	Sí	Sí
AWS: :RDS: DBInstance	Sí	Sí
AWS: :RDS:: Punto final DBProxy	Sí	Sí
AWS: :RDS:: Grupo DBSecurity	Sí	Sí
AWS: :RDS: DBSnapshot	Sí	Sí
AWS: :RDS:: Grupo DBSubnet	Sí	Sí
AWS::RDS::EventSubscription	Sí	Sí
AWS::RDS::Integration	Sí	Sí
AWS::RDS::OptionGroup	Sí	Sí
AWS::Redshift::Cluster	Sí	Sí
AWS::Redshift::ClusterParameterGrupo	Sí	Sí
AWS::Redshift::ClusterSecurityGrupo	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::Redshift::ClusterSnapshot	Sí	Sí
AWS::Redshift::ClusterSubnetGrupo	Sí	Sí
AWS::Redshift::EventSubscription	Sí	Sí
AWS::Redshift::Integration	Sí	Sí
AWS::RolesEn cualquier lugar: :CRL	Sí	Sí
AWS::RolesAnywhere::Profile	Sí	Sí
AWS::RolesAnywhere::TrustAnchor	Sí	Sí
AWS::Route53Profiles::Profile	Sí	Sí
AWS::Route53Profiles::ProfileAssociation	Sí	Sí
AWS::Route53Resolver::FirewallDomainLista	Sí	Sí
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sí	Sí
AWS::Route53Resolver::ResolverEndpoint	Sí	Sí
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Sí	Sí
AWS::Route53Resolver::ResolverRule	Sí	Sí
AWS::Route53Resolver::ResolverRuleAsociación	Sí	Sí
AWS::S3::AccessGrant	Sí	Sí
AWS::S3::AccessGrantsInstancia	Sí	Sí
AWS::S3::AccessGrantsLocation	Sí	Sí
AWS::S3::AccessPoint	Sí	Sí
AWS::S3::AccountPublicAccessBlock	Sí	Sí
AWS::S3::Bucket	Sí	Sí
AWS::S3::StorageLensGrupo	Sí	Sí
AWS::SES::ConfigurationSet	No	Sí
AWS::SES::ContactList	No	Sí
AWS::SES::Template	No	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::SNS::Topic	Sí	Sí
AWS::SQS::Queue	Sí	Sí
AWS::SSM::AssociationCompliance	Sí	Sí
AWS::SSM::Document	Sí	Sí
AWS::SSM::FileData	Sí	Sí
Inventario de AWS::SSM::ManagedInstance	Sí	Sí
AWS::SSM::PatchCompliance	Sí	Sí
AWS::SSM::ResourceDataSincronizar	Sí	Sí
AWS::SageMaker::AppImageConfig	Sí	Sí
AWS::SageMaker::CodeRepository	Sí	Sí
AWS::SageMaker::Domain	Sí	Sí
AWS::SageMaker::EndpointConfig	Sí	Sí
AWS::SageMaker::FeatureGroup	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::SageMaker::Image	Sí	Sí
AWS::SageMaker::Model	Sí	Sí
AWS::SageMaker::MonitoringSchedule	Sí	Sí
AWS::SageMaker::NotebookInstance	Sí	Sí
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sí	Sí
AWS::SageMaker::StudioLifecycleConfig	Sí	Sí
AWS::SageMaker::UserProfile	Sí	Sí
AWS::SecretsManager::ResourcePolicy	Sí	Sí
AWS::SecretsManager::RotationSchedule	Sí	Sí
AWS::SecretsManager::Secret	Sí	Sí
AWS::SecurityHub::Standard	Sí	Sí
AWS::ServiceCatalog::CloudFormationProducto	Sí	Sí
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::ServiceCatalog::Portfolio	Sí	Sí
AWS::ServiceDiscovery::HttpNamespace	Sí	Sí
AWS::ServiceDiscovery::Instance	Sí	Sí
AWS::ServiceDiscovery::PublicDnsEspacio de nombres	Sí	Sí
AWS::ServiceDiscovery::Service	Sí	Sí
AWS::StepFunctions::Activity	Sí	No
AWS::StepFunctions::StateMachine	Sí	Sí
AWS::Transfer::Agreement	Sí	Sí
AWS::Transfer::Certificate	Sí	Sí
AWS::Transfer::Connector	Sí	Sí
AWS::Transfer::Profile	Sí	Sí
AWS::Transfer::Server	Sí	Sí
AWS::Transfer::Workflow	Sí	Sí

Tipo de recurso	China (Pekín)	China (Ningxia)
AWS::WAFRegional::RateBasedRegla	Sí	Sí
AWS::WAFRegional::Rule	Sí	Sí
AWS::WAFRegional::RuleGroup	Sí	Sí
AWS::WAFRegional::WebACL	Sí	Sí
AWS:WAFv2:: IPSet	Sí	Sí
AWS::WAFv2::ManagedRuleSet	Sí	Sí
AWS::WAFv2::RegexPatternSet	Sí	Sí
AWS::WAFv2::RuleGroup	Sí	Sí
AWS::WAFv2::WebACL	Sí	Sí
AWS::WorkSpaces::Workspace	No	Sí

Regiones de África y Oriente Medio

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::ACM::Certificate	Sí	Sí	Sí	Sí
AWS::ACMPCA::CertificateAuthority	Sí	Sí	Sí	Sí
AWS::ACMPCA::CertificateAuthorityActivación	Sí	Sí	Sí	Sí
AWS::APS::RuleGroupsEspacio de nombres	Sí	No	Sí	Sí
AWS::AccessAnalyzer::Analyzer	Sí	Sí	Sí	Sí
AWS::AmazonMQ::Broker	Sí	No	Sí	Sí
AWS::Amplify::App	No	No	Sí	No
AWS::Amplify::Branch	No	No	Sí	No
AWS::ApiGateway::DomainName	Sí	Sí	Sí	Sí
AWS::ApiGateway::Method	Sí	Sí	Sí	Sí
AWS::ApiGateway::RestApi	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::ApiGateway::Stage	Sí	Sí	Sí	Sí
AWS::ApiGateway::UsagePlan	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Api	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Integration	Sí	Sí	Sí	Sí
AWS::ApiGatewayV2::Stage	Sí	Sí	Sí	Sí
AWS::AppConfig::Application	Sí	Sí	Sí	No
AWS::AppConfig::ConfigurationProfile	Sí	Sí	Sí	No
AWS::AppConfig::DeploymentStrategy	Sí	Sí	Sí	Sí
AWS::AppConfig::Environment	Sí	Sí	Sí	No
AWS::AppConfig::Extension	Sí	Sí	Sí	Sí
AWS::AppConfig::ExtensionAssociation	Sí	Sí	Sí	Sí
AWS::AppConfig::HostedConfigurationVersión	Sí	Sí	Sí	No

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::AppFlow::Flow	Sí	No	No	No
AWS::AppIntegrations::Application	Sí	No	No	No
AWS::AppIntegrations::DataIntegration	Sí	No	No	No
AWS::AppIntegrations::EventIntegration	Sí	No	No	No
AWS::AppMesh::GatewayRoute	Sí	Sí	Sí	No
AWS::AppMesh::Mesh	Sí	Sí	Sí	No
AWS::AppMesh::Route	Sí	Sí	Sí	No
AWS::AppMesh::VirtualGateway	Sí	Sí	Sí	No
AWS::AppMesh::VirtualNode	Sí	Sí	Sí	No
AWS::AppMesh::VirtualRouter	Sí	Sí	Sí	No
AWS::AppMesh::VirtualService	Sí	Sí	Sí	No
AWS::AppSync::Api	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::AppSync::ApiCache	Sí	Sí	Sí	Sí
AWS::AppSync::GraphQLApi	Sí	Sí	Sí	Sí
AWS::Athena::DataCatalog	Sí	Sí	Sí	Sí
AWS::Athena::PreparedStatement	Sí	Sí	Sí	Sí
AWS::Athena::WorkGroup	Sí	Sí	Sí	Sí
AWS::AutoScaling::AutoScalingGrupo	Sí	Sí	Sí	Sí
AWS::AutoScaling::LaunchConfiguration	Sí	Sí	Sí	Sí
AWS::AutoScaling::ScalingPolicy	Sí	Sí	Sí	Sí
AWS::AutoScaling::ScheduledAction	Sí	Sí	Sí	Sí
AWS::AutoScaling::WarmPool	Sí	No	Sí	No
AWS::Backup::BackupPlan	Sí	Sí	Sí	Sí
AWS::Backup::BackupSelection	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::Backup::BackupVault	Sí	Sí	Sí	Sí
AWS::Backup::RecoveryPoint	Sí	Sí	Sí	Sí
AWS::Backup::ReportPlan	Sí	No	Sí	Sí
AWS::Backup::RestoreTestingPlan	Sí	No	Sí	Sí
AWS::BackupGateway::Hypervisor	Sí	No	Sí	No
AWS::Batch::ComputeEnvironment	Sí	No	Sí	Sí
AWS::Batch::JobQueue	Sí	No	Sí	Sí
AWS::Batch::SchedulingPolicy	Sí	Sí	Sí	Sí
AWS::Bedrock::Guardrail	No	No	No	Sí
AWS::Cassandra::Keyspace	No	No	Sí	No
AWS::Cloud9::EnvironmentEC2	Sí	No	Sí	No
AWS::CloudFormation::GuardHook	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::CloudFormation::LambdaHook	Sí	Sí	Sí	Sí
AWS::CloudFormation::Stack	Sí	No	Sí	No
AWS::CloudFormation::StackSet	Sí	Sí	Sí	Sí
AWS::CloudTrail::EventDataTienda	Sí	Sí	Sí	Sí
AWS::CloudTrail::Trail	Sí	Sí	Sí	Sí
AWS::CloudWatch::Alarm	Sí	Sí	Sí	Sí
AWS::CloudWatch::MetricStream	Sí	Sí	Sí	Sí
AWS::CodeBuild::Project	Sí	Sí	Sí	Sí
AWS::CodeBuild::ReportGroup	Sí	Sí	Sí	Sí
AWS::CodeDeploy::Application	Sí	No	Sí	No
AWS::CodeDeploy::DeploymentConfig	Sí	No	Sí	No
AWS::CodeDeploy::DeploymentGroup	Sí	No	Sí	No

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::CodePipeline::Pipeline	No	Sí	No	Sí
AWS::Cognito::IdentityPool	Sí	Sí	Sí	Sí
AWS::Cognito::UserPool	Sí	Sí	Sí	Sí
AWS::Cognito::UserPoolCliente	Sí	Sí	Sí	Sí
AWS::Cognito::UserPoolGrupo	Sí	Sí	Sí	Sí
AWS::Config::AggregationAuthorization	Sí	Sí	Sí	Sí
AWS::Config::ConfigurationRecorder	Sí	Sí	Sí	Sí
AWS::Config::ConformancePack	Sí	Sí	Sí	Sí
Conformidad de AWS::Conf ig::ConformancePack	Sí	Sí	Sí	Sí
AWS::Config::ResourceCompliance	Sí	Sí	Sí	Sí
AWS::Config::StoredQuery	Sí	Sí	Sí	Sí
AWS::Connect::Instance	Sí	No	No	No

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::Connect::PhoneNumber	Sí	No	No	No
AWS::Connect::QuickConnect	Sí	No	No	No
AWS::Connect::Rule	Sí	No	No	No
AWS::Connect::SecurityProfile	Sí	No	No	No
AWS::Connect::User	Sí	No	No	No
AWS::CustomerProfiles::Domain	Sí	No	No	No
AWS::CustomerProfiles::ObjectType	Sí	No	No	No
AWS::DMS::Certificate	Sí	No	Sí	No
AWS::DMS::Endpoint	Sí	No	Sí	No
AWS::DMS::EventSubscription	Sí	No	Sí	No
AWS::DMS::MigrationProject	Sí	Sí	Sí	Sí
AWS::DMS::ReplicationInstance	Sí	No	Sí	No

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::DMS::ReplicationSubnetGrupo	Sí	No	Sí	No
AWS::DMS::ReplicationTask	Sí	No	Sí	No
AWS::DataSync::Agent	Sí	Sí	Sí	Sí
AWS::DataSync::LocationEFS	Sí	No	Sí	Sí
AWS::DataSync::LocationFSxLustre	Sí	No	Sí	Sí
AWS::DataSync::LocationFSxVentanas	Sí	No	Sí	No
AWS::DataSync::LocationHDFS	Sí	No	Sí	Sí
AWS::DataSync::LocationNFS	Sí	No	Sí	Sí
AWS::DataSync::LocationObjectAlmacenamiento	Sí	No	Sí	Sí
AWS::DataSync::LocationS3	Sí	Sí	Sí	Sí
AWS::DataSync::LocationSMB	Sí	No	Sí	Sí
AWS::DataSync::Task	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::Detective::Graph	Sí	Sí	Sí	No
AWS::DynamoDB::Table	Sí	Sí	Sí	Sí
AWS::EC2::CapacityReservation	Sí	Sí	Sí	Sí
AWS::EC2::ClientVpnPunto final	Sí	No	Sí	Sí
AWS::EC2::ClientVpnTargetNetworkAssociation	Sí	Sí	Sí	Sí
AWS::EC2::CustomerGateway	Sí	Sí	Sí	Sí
AWS:EC2:: DHCPOptions	Sí	Sí	Sí	Sí
AWS::EC2: EC2 Flota	Sí	No	Sí	Sí
AWS:EC2: :EIP	Sí	Sí	Sí	Sí
AWS:EC2:: EIPAssociation	Sí	Sí	Sí	Sí
AWS::EC2::EgressOnlyInternetGateway	Sí	No	Sí	Sí
AWS::EC2::FlowLog	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::EC2::Host	Sí	Sí	Sí	Sí
AWS:EC2: :IPAM	Sí	No	Sí	Sí
AWS:EC2:: IPAMPool	Sí	No	Sí	Sí
AWS:EC2: IPAMPool Cir	Sí	Sí	Sí	Sí
AWS::EC2: IPAMResource Descubrimiento	Sí	Sí	Sí	Sí
AWS:EC2:: IPAMResou rce DiscoveryAssociation	Sí	Sí	Sí	Sí
AWS:EC2:: IPAMScope	Sí	No	Sí	Sí
AWS::EC2::Instance	Sí	Sí	Sí	Sí
AWS::EC2::InstanceConnectPunto final	Sí	Sí	Sí	Sí
AWS::EC2::InternetGateway	Sí	Sí	Sí	Sí
AWS::EC2::LaunchTemplate	Sí	No	Sí	No
AWS::EC2::NatGateway	Sí	No	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::EC2::NetworkAcl	Sí	Sí	Sí	Sí
AWS::EC2::NetworkInsightsAccessScope	Sí	No	Sí	Sí
AWS::EC2::NetworkI nsightsAccessScopeAnalysis	Sí	No	Sí	Sí
AWS::EC2::NetworkInsightsAnálisis	Sí	No	Sí	No
AWS::EC2::NetworkInsightsRuta	Sí	No	Sí	Sí
AWS::EC2::NetworkInterface	Sí	Sí	Sí	Sí
AWS::EC2::PrefixList	Sí	Sí	Sí	Sí
AWS::EC2::RouteTable	Sí	Sí	Sí	Sí
AWS::EC2::SecurityGroup	Sí	Sí	Sí	Sí
AWS::EC2::SecurityGroupVpcAssociation	Sí	Sí	Sí	Sí
AWS::EC2::SnapshotBlockPublicAccess	Sí	Sí	Sí	Sí
AWS::EC2::SpotFleet	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::EC2::Subnet	Sí	Sí	Sí	Sí
AWS::EC2::SubnetCidrBloquear	Sí	Sí	Sí	Sí
AWS::EC2::SubnetNetworkAclAssociation	Sí	Sí	Sí	Sí
AWS::EC2::SubnetRouteTableAssociation	Sí	Sí	Sí	Sí
AWS::EC2::TrafficMirrorFiltro	Sí	Sí	Sí	Sí
AWS::EC2::TrafficMirrorSession	Sí	No	Sí	Sí
AWS::EC2::TrafficMirrorObjetivo	Sí	No	Sí	Sí
AWS::EC2::TransitGateway	Sí	Sí	Sí	Sí
AWS::EC2::TransitGatewayAdjunto	Sí	No	Sí	Sí
AWS::EC2::TransitGatewayConnect	Sí	No	Sí	Sí
AWS::EC2::TransitGatewayMulticastDomain	Sí	Sí	Sí	Sí
AWS::EC2::TransitGatewayRouteTable	Sí	No	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS:EC2: :VPC	Sí	Sí	Sí	Sí
AWS:EC2:: VPCBlock PublicAccessExclusion	Sí	Sí	Sí	Sí
AWS:EC2:: VPCBlock PublicAccessOptions	Sí	Sí	Sí	Sí
AWS:EC2:: VPCEndpoint	Sí	Sí	Sí	Sí
AWS:EC2:: VPCEndpoi nt ConnectionNotification	Sí	Sí	Sí	Sí
AWS:EC2:: VPCEndpoint Servicio	Sí	Sí	Sí	Sí
AWS:EC2:: VPCGateway Adjunto	Sí	Sí	Sí	Sí
AWS:EC2:: VPCPeering Conexión	Sí	Sí	Sí	Sí
AWS:EC2:: VPNConnection	Sí	Sí	Sí	Sí
AWS:EC2:: VPNConnection Ruta	Sí	Sí	Sí	Sí
AWS:EC2:: VPNGateway	Sí	Sí	Sí	Sí
AWS::EC2::VerifiedAccessInstancia	No	Sí	No	No

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::EC2::Volume	Sí	Sí	Sí	Sí
AWS::ECR::PullThroughCacheRule	Sí	Sí	Sí	Sí
AWS::ECR::RegistryPolicy	Sí	Sí	Sí	Sí
AWS::ECR::ReplicationConfiguration	Sí	Sí	Sí	Sí
AWS::ECR::Repository	Sí	Sí	Sí	Sí
AWS::ECR::RepositoryCreationPlantilla	Sí	Sí	Sí	Sí
AWS::ECS::CapacityProvider	Sí	Sí	Sí	Sí
AWS::ECS::Cluster	Sí	Sí	Sí	Sí
AWS::ECS::Service	Sí	Sí	Sí	Sí
AWS::ECS::TaskDefinition	Sí	Sí	Sí	Sí
AWS::ECS::TaskSet	Sí	No	Sí	Sí
AWS::EFS::AccessPoint	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::EFS::FileSystem	Sí	Sí	Sí	Sí
AWS::EKS::Addon	Sí	No	Sí	Sí
AWS::EKS::Cluster	Sí	Sí	Sí	Sí
AWS::EKS::FargateProfile	Sí	Sí	Sí	Sí
AWS::EKS::IdentityProviderConfig	Sí	No	Sí	Sí
AWS::EMR::SecurityConfiguration	Sí	Sí	Sí	Sí
AWS::EMR::Studio	Sí	Sí	Sí	Sí
AWS::EMRContainers::VirtualCluster	Sí	Sí	Sí	Sí
AWS::EMRServerless::Application	Sí	No	Sí	Sí
AWS::ElasticBeanstalk::Application	Sí	No	Sí	Sí
AWS::ElasticBeanstalk::ApplicationVersion	Sí	No	Sí	Sí
AWS::ElasticBeanstalk::Environment	Sí	No	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::ElasticLoadBalancing::LoadBalancer	Sí	Sí	Sí	Sí
AWS::ElasticLoadBalancingV2::Listener	Sí	No	Sí	Sí
AWS::ElasticLoadBalancingV2::LoadBalancer	Sí	Sí	Sí	Sí
AWS::ElasticLoadBalancingV2::TargetGroup	Sí	Sí	Sí	Sí
AWS::Elasticsearch::Domain	Sí	Sí	Sí	Sí
AWS::EntityResolution::IdMappingflujo de trabajo	Sí	No	No	No
AWS::EntityResolution::MatchingWorkflow	Sí	No	No	No
AWS::EntityResolution::SchemaMapping	Sí	No	No	No
AWS::EventSchemas::Discoverer	Sí	No	Sí	Sí
AWS::EventSchemas::Registry	Sí	No	Sí	Sí
AWS::EventSchemas::RegistryPolicy	Sí	No	Sí	Sí
AWS::EventSchemas::Schema	Sí	No	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::Events::ApiDestination	Sí	No	Sí	Sí
AWS::Events::Archive	Sí	No	Sí	Sí
AWS::Events::Connection	Sí	No	Sí	Sí
AWS::Events::EventBus	Sí	Sí	Sí	Sí
AWS::Events::Rule	Sí	No	Sí	No
AWS::FIS::ExperimentTemplate	Sí	No	Sí	No
AWS::Glue::Classifier	Sí	Sí	Sí	Sí
AWS::Glue::Database	Sí	No	Sí	Sí
AWS::Glue::Job	Sí	Sí	Sí	Sí
AWS::Glue::MLTransform	Sí	Sí	Sí	Sí
AWS::Glue::Registry	Sí	No	Sí	No
AWS::GroundStation::Config	Sí	No	Sí	No

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::GroundStation ::DataflowEndpointGrupo	Sí	No	Sí	No
AWS::GroundStation::MissionProfile	Sí	No	Sí	No
AWS::GuardDuty::Detector	Sí	Sí	Sí	Sí
AWS::GuardDuty::Filter	Sí	No	Sí	No
AWS::GuardDeber: IPSet	Sí	No	Sí	Sí
AWS::GuardDuty::MalwareProtectionPlan	Sí	Sí	Sí	Sí
AWS::GuardDuty::ThreatIntelSet	Sí	Sí	Sí	Sí
AWS::IAM::Group	Sí	No	Sí	No
AWS::IAM::Policy	Sí	No	Sí	No
AWS::IAM::Role	Sí	No	Sí	No
AWS::IAM::User	Sí	No	Sí	No
AWS::ImageBuilder::ContainerRecipe	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::ImageBuilder::DistributionConfiguration	Sí	Sí	Sí	Sí
AWS::ImageBuilder::ImagePipeline	Sí	Sí	Sí	Sí
AWS::ImageBuilder::ImageRecipe	Sí	Sí	Sí	Sí
AWS::ImageBuilder::InfrastructureConfiguration	Sí	Sí	Sí	Sí
AWS::ImageBuilder::LifecyclePolicy	Sí	No	Sí	Sí
AWS::InspectorV2::Activation	Sí	Sí	Sí	Sí
AWS::InspectorV2::Filter	Sí	No	Sí	Sí
AWS::IoT::AccountAuditConfiguración	No	No	Sí	Sí
AWS::IoT::Authorizer	No	No	Sí	Sí
AWS::IoT:: CACertificate	No	No	Sí	Sí
AWS::IoT::CustomMetric	No	No	Sí	Sí
AWS::IoT::Dimension	No	No	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::IoT::DomainConfiguration	No	No	Sí	Sí
AWS::IoT::FleetMetric	No	No	Sí	Sí
AWS::IoT::JobTemplate	No	No	Sí	Sí
AWS::IoT::MitigationAction	No	No	Sí	Sí
AWS::IoT::Policy	No	No	Sí	Sí
AWS::IoT::ProvisioningTemplate	No	No	Sí	Sí
AWS::IoT::RoleAlias	No	No	Sí	Sí
AWS::IoT::ScheduledAudit	No	No	Sí	Sí
AWS::IoT::SecurityProfile	No	No	Sí	Sí
AWS::IoT::ThingGroup	No	No	Sí	Sí
AWS::KMS::Alias	Sí	No	Sí	Sí
AWS::KMS::Key	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::KafkaConnect::CustomPlugin	Sí	No	Sí	Sí
AWS::Kinesis::Stream	Sí	No	Sí	Sí
AWS::Kinesis::StreamConsumer	Sí	Sí	Sí	Sí
AWS::KinesisAnalyticsV2::Application	Sí	Sí	Sí	Sí
AWS::KinesisFirehose::DeliveryStream	Sí	Sí	Sí	Sí
AWS::KinesisVideo::SignalingChannel	No	No	Sí	No
AWS::KinesisVideo::Stream	No	No	Sí	No
AWS::Lambda::CodeSigningConfig	Sí	No	Sí	No
AWS::Lambda::Function	Sí	Sí	Sí	Sí
AWS::Lex::Bot	Sí	No	No	No
AWS::Lex::BotAlias	Sí	No	No	No
AWS::Logs::Destination	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::MSK::BatchScramSecreto	Sí	No	Sí	Sí
AWS::MSK::Cluster	Sí	No	Sí	Sí
AWS::MSK::ClusterPolicy	Sí	Sí	Sí	Sí
AWS::MSK::Configuration	Sí	Sí	Sí	Sí
AWS::MSK::VpcConnection	Sí	Sí	Sí	Sí
AWS::Macie::Session	Sí	Sí	Sí	No
AWS::MediaConnect::FlowEntitlement	Sí	No	No	Sí
AWS::MediaConnect::FlowSource	Sí	No	No	Sí
AWS::MediaConnect::FlowVpcInterfaz	Sí	No	No	Sí
AWS::MediaConnect::Gateway	Sí	No	No	No
AWS::MediaLive::Multiplexprogram	No	No	No	Sí
AWS::MediaPackage::Asset	No	No	No	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::MediaPackage::PackagingConfiguration	No	No	No	Sí
AWS::MediaPackage::PackagingGroup	No	No	No	Sí
AWS::MediaPackageV2::Channel	No	No	No	Sí
AWS::MediaPackageV2::ChannelGroup	No	No	No	Sí
AWS::MediaPackageV2::OriginEndpoint	No	No	No	Sí
AWS::MediaTailor::LiveSource	Sí	No	No	Sí
AWS::MediaTailor::PlaybackConfiguration	Sí	No	No	Sí
AWS::NetworkFirewall::Firewall	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::FirewallPolicy	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::RuleGroup	Sí	Sí	Sí	Sí
AWS::NetworkFirewall:TLSInspection Configuración	Sí	Sí	Sí	Sí
AWS::NetworkFirewall::VpcEndpointAsociación	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::Omics::RunGroup	No	Sí	No	No
AWS::Omics::Workflow	No	Sí	No	No
AWS::OpenSearch::Domain	Sí	No	Sí	No
AWS::PCAConnectorAD::Connector	Sí	Sí	Sí	Sí
AWS::PCAConnectorAD::DirectoryRegistration	Sí	Sí	Sí	Sí
AWS::QuickSight::Dashboard	Sí	No	No	No
AWS: :RDS: DBCluster	Sí	Sí	Sí	Sí
AWS: :RDS:: Instantánea DBCluster	Sí	No	Sí	Sí
AWS: :RDS: DBInstance	Sí	Sí	Sí	Sí
AWS: :RDS:: Punto final DBProxy	Sí	Sí	Sí	Sí
AWS: :RDS:: Grupo DBSecurity	Sí	Sí	Sí	Sí
AWS: :RDS: DBSnapshot	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS: :RDS:: Grupo DBSubnet	Sí	Sí	Sí	Sí
AWS::RDS::EventSubscription	Sí	Sí	Sí	Sí
AWS::RDS::GlobalCluster	Sí	Sí	Sí	Sí
AWS::RDS::Integration	Sí	Sí	Sí	Sí
AWS::RDS::OptionGroup	Sí	Sí	Sí	Sí
AWS::RUM::AppMonitor	Sí	No	Sí	Sí
AWS::Redshift::Cluster	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterParameterGrupo	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSecurityGrupo	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSnapshot	Sí	Sí	Sí	Sí
AWS::Redshift::ClusterSubnetGrupo	Sí	Sí	Sí	Sí
AWS::Redshift::EndpointAccess	Sí	No	Sí	No

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::Redshift::EndpointAuthorization	Sí	No	Sí	No
AWS::Redshift::EventSubscription	Sí	Sí	Sí	Sí
AWS::Redshift::Integration	Sí	Sí	Sí	Sí
AWS::Redshift::ScheduledAction	No	No	Sí	No
AWS::ResilienceHub::App	Sí	No	Sí	No
AWS::ResilienceHub::ResiliencyPolicy	Sí	No	Sí	No
AWS::ResourceExplorer2::Index	Sí	No	Sí	Sí
AWS::RolesEn cualquier lugar: :CRL	Sí	Sí	Sí	Sí
AWS::RolesAnywhere::Profile	Sí	Sí	Sí	Sí
AWS::RolesAnywhere::TrustAnchor	Sí	Sí	Sí	Sí
AWS::Route53Profiles::Profile	Sí	Sí	Sí	Sí
AWS::Route53Profiles::ProfileAssociation	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::Route53Resolver::FirewallDomainLista	Sí	No	Sí	No
AWS::Route53Resolver::FirewallRuleGrupo	Sí	No	Sí	No
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverEndpoint	Sí	No	Sí	Sí
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Sí	Sí	Sí	Sí
AWS::Route53Resolver::ResolverRule	Sí	No	Sí	Sí
AWS::Route53Resolver::ResolverRuleAsociación	Sí	No	Sí	Sí
AWS::S3::AccessGrant	Sí	Sí	Sí	Sí
AWS::S3::AccessGrantsInstancia	Sí	Sí	Sí	Sí
AWS::S3::AccessGrantsLocation	Sí	Sí	Sí	Sí
AWS::S3::AccessPoint	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::S3::AccountPublicAccessBlock	Sí	No	Sí	Sí
AWS::S3::Bucket	Sí	Sí	Sí	Sí
AWS::S3Tables::TableBucket	Sí	Sí	Sí	Sí
AWS::S3Tables::TableBucketPolítica	Sí	Sí	Sí	Sí
AWS::SES::ConfigurationSet	Sí	Sí	Sí	Sí
AWS::SES::ContactList	Sí	Sí	Sí	Sí
AWS::SES::DedicatedIpPiscina	Sí	Sí	Sí	Sí
AWS::SES::MailManagerTrafficPolicy	Sí	No	Sí	Sí
AWS::SES::ReceiptFilter	Sí	No	Sí	No
AWS::SES::ReceiptRuleSet	Sí	No	Sí	No
AWS::SES::Template	Sí	Sí	Sí	Sí
AWS::SNS::Topic	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::SQS::Queue	Sí	No	Sí	No
AWS::SSM::AssociationCompliance	Sí	Sí	Sí	Sí
AWS::SSM::Document	Sí	Sí	Sí	Sí
AWS::SSM::FileData	Sí	Sí	Sí	Sí
Inventario de AWS::SSM::ManagedInstance	Sí	Sí	Sí	Sí
AWS::SSM::PatchCompliance	Sí	Sí	Sí	Sí
AWS::SSM::ResourceDataSincronizar	Sí	Sí	Sí	Sí
AWS::SageMaker::AppImageConfig	Sí	Sí	Sí	Sí
AWS::SageMaker::CodeRepository	Sí	No	Sí	No
AWS::SageMaker::DataQualityJobDefinition	No	No	Sí	No
AWS::SageMaker::Domain	Sí	No	Sí	No
AWS::SageMaker::EndpointConfig	Sí	No	Sí	No

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::SageMaker::FeatureGroup	Sí	Sí	Sí	No
AWS::SageMaker::Image	Sí	Sí	Sí	Sí
AWS::SageMaker::InferenceExperiment	Sí	No	Sí	No
AWS::SageMaker::MlflowTrackingServidor	Sí	Sí	Sí	Sí
AWS::SageMaker::Model	Sí	No	Sí	No
AWS::SageMaker::ModelBiasJobDefinition	No	No	Sí	No
AWS::SageMaker::ModelExplainabilityJobDefinition	No	No	Sí	No
AWS::SageMaker::ModelQualityJobDefinition	No	No	Sí	No
AWS::SageMaker::MonitoringSchedule	No	No	Sí	No
AWS::SageMaker::NotebookInstance	Sí	No	Sí	No
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sí	No	Sí	No
AWS::SageMaker::StudioLifecycleConfig	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::SageMaker::UserProfile	Sí	Sí	Sí	Sí
AWS::SecretsManager::ResourcePolicy	Sí	Sí	Sí	Sí
AWS::SecretsManager::RotationSchedule	Sí	Sí	Sí	Sí
AWS::SecretsManager::Secret	Sí	Sí	Sí	Sí
AWS::SecurityHub::Standard	Sí	Sí	Sí	Sí
AWS::ServiceCatalog::CloudFormationProducto	Sí	No	Sí	Sí
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sí	No	Sí	Sí
AWS::ServiceCatalog::Portfolio	Sí	No	Sí	Sí
AWS::ServiceDiscovery::HttpNamespace	Sí	Sí	Sí	Sí
AWS::ServiceDiscovery::Instance	Sí	No	Sí	Sí
AWS::ServiceDiscovery::PublicDnsEspacio de nombres	Sí	Sí	Sí	Sí
AWS::ServiceDiscovery::Service	Sí	No	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::ShieldRegional::Protection	Sí	Sí	Sí	Sí
AWS::Signer::SigningProfile	Sí	No	Sí	No
AWS::StepFunctions::Activity	Sí	Sí	Sí	Sí
AWS::StepFunctions::StateMachine	Sí	Sí	Sí	Sí
AWS::Transfer::Agreement	Sí	No	Sí	Sí
AWS::Transfer::Certificate	Sí	Sí	Sí	Sí
AWS::Transfer::Connector	Sí	Sí	Sí	Sí
AWS::Transfer::Profile	Sí	Sí	Sí	Sí
AWS::Transfer::Server	Sí	Sí	Sí	Sí
AWS::Transfer::Workflow	Sí	Sí	Sí	Sí
AWS::WAFRegional::RateBasedRegla	Sí	Sí	Sí	Sí
AWS::WAFRegional::Rule	Sí	Sí	Sí	Sí

Tipo de recurso	África (Ciudad del Cabo)	Israel (Tel Aviv)	Medio Oriente (Baréin)	Medio Oriente (EAU)
AWS::WAFRegional::RuleGroup	Sí	Sí	Sí	Sí
AWS::WAFRegional::WebACL	Sí	Sí	Sí	Sí
AWS:WAFv2:: IPSet	Sí	Sí	Sí	Sí
AWS::WAFv2::ManagedRuleSet	Sí	Sí	Sí	Sí
AWS::WAFv2::RegexPatternSet	Sí	Sí	Sí	Sí
AWS::WAFv2::RuleGroup	Sí	Sí	Sí	Sí
AWS::WAFv2::WebACL	Sí	Sí	Sí	Sí
AWS::WorkSpaces::Workspace	Sí	No	No	No
AWS::XRay::EncryptionConfig	Sí	Sí	No	Sí

GovCloud Regiones

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::ACM::Certificate	Sí	Sí
AWS::ACMPCA::CertificateAuthority	Sí	Sí
AWS::ACMPCA::CertificateAuthorityActivación	Sí	Sí
AWS::AccessAnalyzer::Analyzer	Sí	Sí
AWS::AmazonMQ::Broker	Sí	Sí
AWS::ApiGateway::DomainName	Sí	Sí
AWS::ApiGateway::Method	Sí	Sí
AWS::ApiGateway::RestApi	Sí	Sí
AWS::ApiGateway::Stage	Sí	Sí
AWS::ApiGateway::UsagePlan	Sí	Sí
AWS::ApiGatewayV2::Api	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::ApiGatewayV2::Integration	Sí	Sí
AWS::ApiGatewayV2::Stage	Sí	Sí
AWS::AppConfig::Application	Sí	Sí
AWS::AppConfig::ConfigurationProfile	Sí	Sí
AWS::AppConfig::DeploymentStrategy	Sí	Sí
AWS::AppConfig::Environment	Sí	Sí
AWS::AppConfig::Extension	Sí	Sí
AWS::AppConfig::ExtensionAssociation	Sí	Sí
AWS::AppConfig::HostedConfigurationVersión	Sí	Sí
AWS::AppStream::AppBlockConstructor	Sí	Sí
AWS::AppStream::Application	Sí	Sí
AWS::AppStream::DirectoryConfig	Sí	No

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::AppStream::Fleet	Sí	No
AWS::AppStream::Stack	Sí	No
AWS::Athena::DataCatalog	Sí	Sí
AWS::Athena::WorkGroup	Sí	Sí
AWS::AutoScaling::AutoScalingGrupo	Sí	Sí
AWS::AutoScaling::LaunchConfiguration	Sí	Sí
AWS::AutoScaling::ScalingPolicy	Sí	Sí
AWS::AutoScaling::ScheduledAction	Sí	Sí
AWS::AutoScaling::WarmPool	Sí	Sí
AWS::Backup::BackupPlan	Sí	Sí
AWS::Backup::BackupSelection	Sí	Sí
AWS::Backup::BackupVault	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::Backup::RecoveryPoint	Sí	Sí
AWS::BackupGateway::Hypervisor	Sí	Sí
AWS::Batch::ComputeEnvironment	Sí	Sí
AWS::Batch::JobQueue	Sí	Sí
AWS::Batch::SchedulingPolicy	Sí	Sí
AWS::Bedrock::Guardrail	Sí	Sí
AWS::Bedrock::KnowledgeBase	Sí	Sí
AWS::Bedrock::Prompt	Sí	Sí
AWS::Cassandra::Keyspace	Sí	Sí
AWS::CloudFormation::Stack	Sí	Sí
AWS::CloudFormation::StackSet	Sí	Sí
AWS::CloudTrail::EventDataTienda	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::CloudTrail::Trail	Sí	Sí
AWS::CloudWatch::Alarm	Sí	Sí
AWS::CodeBuild::Project	Sí	Sí
AWS::CodeBuild::ReportGroup	Sí	Sí
AWS::Cognito::IdentityPool	Sí	No
AWS::Cognito::UserPoolGrupo	Sí	No
AWS::Config::ConfigurationRecorder	Sí	Sí
AWS::Config::ConformancePack	Sí	Sí
Conformidad de AWS::Config::ConformancePack	Sí	Sí
AWS::Config::ResourceCompliance	Sí	Sí
AWS::Config::StoredQuery	Sí	Sí
AWS::Connect::Instance	Sí	No

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::Connect::QuickConnect	Sí	No
AWS::Connect::SecurityProfile	Sí	No
AWS::Connect::User	Sí	No
AWS::DMS::Certificate	Sí	Sí
AWS::DMS::Endpoint	Sí	Sí
AWS::DMS::EventSubscription	Sí	Sí
AWS::DMS::ReplicationInstance	Sí	Sí
AWS::DMS::ReplicationSubnetGrupo	Sí	Sí
AWS::DMS::ReplicationTask	Sí	Sí
AWS::DataSync::Agent	Sí	Sí
AWS::DataSync::LocationEFS	Sí	Sí
AWS::DataSync::LocationFSxLustre	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::DataSync::LocationFSxVentanas	Sí	Sí
AWS::DataSync::LocationHDFS	Sí	Sí
AWS::DataSync::LocationNFS	Sí	Sí
AWS::DataSync::LocationObjectAlmacenamiento	Sí	Sí
AWS::DataSync::LocationS3	Sí	Sí
AWS::DataSync::LocationSMB	Sí	Sí
AWS::DataSync::Task	Sí	Sí
AWS::Detective::Graph	Sí	Sí
AWS::DynamoDB::Table	Sí	Sí
AWS::EC2::CapacityReservation	Sí	Sí
AWS::EC2::ClientVpnPunto final	Sí	Sí
AWS::EC2::ClientVpnTargetNetworkAssociation	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::EC2::CustomerGateway	Sí	Sí
AWS:EC2:: DHCPOptions	Sí	Sí
AWS::EC2: EC2 Flota	Sí	Sí
AWS:EC2: :EIP	Sí	Sí
AWS::EC2::EgressOnlyInternetGateway	Sí	Sí
AWS::EC2::FlowLog	Sí	Sí
AWS::EC2::Host	Sí	Sí
AWS:EC2: :IPAM	Sí	Sí
AWS:EC2:: IPAMPool	Sí	Sí
AWS:EC2: IPAMPool Cir	Sí	Sí
AWS::EC2: IPAMResource Descubrimiento	Sí	Sí
AWS:EC2:: IPAMResource DiscoveryAssociation	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS:EC2:: IPAMScope	Sí	Sí
AWS::EC2::Instance	Sí	Sí
AWS::EC2::InstanceConnectPunto final	Sí	Sí
AWS::EC2::InternetGateway	Sí	Sí
AWS::EC2::LaunchTemplate	Sí	Sí
AWS::EC2::NatGateway	Sí	Sí
AWS::EC2::NetworkAcl	Sí	Sí
AWS::EC2::NetworkInterface	Sí	Sí
AWS::EC2::PrefixList	Sí	Sí
AWS::EC2::RouteTable	Sí	Sí
AWS::EC2::SecurityGroup	Sí	Sí
AWS::EC2::SecurityGroupVpcAssociation	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::EC2::SnapshotBlockPublicAccess	Sí	Sí
AWS::EC2::SpotFleet	Sí	Sí
AWS::EC2::Subnet	Sí	Sí
AWS::EC2::SubnetCidrBloquear	Sí	Sí
AWS::EC2::SubnetNetworkAclAssociation	Sí	Sí
AWS::EC2::SubnetRouteTableAssociation	Sí	Sí
AWS::EC2::TrafficMirrorFiltro	Sí	Sí
AWS::EC2::TrafficMirrorSession	Sí	Sí
AWS::EC2::TrafficMirrorObjetivo	Sí	Sí
AWS::EC2::TransitGateway	Sí	No
AWS::EC2::TransitGatewayAdjunto	Sí	Sí
AWS::EC2::TransitGatewayConnect	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::EC2::TransitGatewayMulticastDomain	Sí	Sí
AWS::EC2::TransitGatewayRouteTable	Sí	Sí
AWS:EC2: :VPC	Sí	Sí
AWS:EC2:: VPCBlock PublicAccessExclusion	Sí	Sí
AWS:EC2:: VPCBlock PublicAccessOptions	Sí	Sí
AWS:EC2:: VPCEndpoint	Sí	Sí
AWS:EC2:: VPCEndpoint ConnectionNotification	Sí	Sí
AWS:EC2:: VPCEndpoint Servicio	Sí	No
AWS:EC2:: VPCGateway Adjunto	Sí	Sí
AWS:EC2:: VPCPeering Conexión	Sí	Sí
AWS:EC2:: VPNConnection	Sí	Sí
AWS:EC2:: VPNConnection Ruta	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS:EC2:: VPNGateway	Sí	Sí
AWS::EC2::VerifiedAccessInstancia	Sí	Sí
AWS::EC2::Volume	Sí	Sí
AWS::ECR::ReplicationConfiguration	Sí	Sí
AWS::ECR::Repository	Sí	Sí
AWS::ECS::CapacityProvider	Sí	Sí
AWS::ECS::Cluster	Sí	Sí
AWS::ECS::Service	Sí	Sí
AWS::ECS::TaskDefinition	Sí	Sí
AWS::ECS::TaskSet	Sí	Sí
AWS::EFS::AccessPoint	Sí	Sí
AWS::EFS::FileSystem	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::EKS::Addon	Sí	Sí
AWS::EKS::Cluster	Sí	Sí
AWS::EKS::IdentityProviderConfig	Sí	Sí
AWS::EMR::SecurityConfiguration	Sí	Sí
AWS::EMR::Studio	Sí	Sí
AWS::EMRContainers::VirtualCluster	Sí	Sí
AWS::ElasticBeanstalk::Application	Sí	Sí
AWS::ElasticBeanstalk::ApplicationVersion	Sí	Sí
AWS::ElasticBeanstalk::Environment	Sí	Sí
AWS::ElasticLoadBalancing::LoadBalancer	Sí	Sí
AWS::ElasticLoadBalancingV2::Listener	Sí	Sí
AWS::ElasticLoadBalancingV2::LoadBalancer	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::ElasticLoadBalancingV2::TargetGroup	Sí	Sí
AWS::Elasticsearch::Domain	Sí	Sí
AWS::Events::EventBus	Sí	Sí
AWS::Events::Rule	Sí	Sí
AWS::FIS::ExperimentTemplate	Sí	Sí
AWS::Glue::Classifier	Sí	Sí
AWS::Glue::Job	Sí	Sí
AWS::Glue::MLTransform	Sí	No
AWS::Glue::Registry	Sí	Sí
AWS::GreengrassV2::ComponentVersion	Sí	Sí
AWS::GuardDuty::Detector	Sí	Sí
AWS::GuardDuty::Filter	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::GuardDeber: IPSet	Sí	Sí
AWS::GuardDuty::ThreatIntelSet	Sí	Sí
AWS::IAM::Group	Sí	Sí
AWS::IAM::InstanceProfile	No	Sí
AWS: :IAM:: OIDCProvider	No	Sí
AWS::IAM::Policy	Sí	Sí
AWS::IAM::Role	Sí	Sí
AWS: :IAM:: SAMLProvider	No	Sí
AWS::IAM::ServerCertificate	No	Sí
AWS::IAM::User	Sí	Sí
AWS::ImageBuilder::ContainerRecipe	Sí	Sí
AWS::ImageBuilder::DistributionConfiguration	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::ImageBuilder::ImagePipeline	Sí	Sí
AWS::ImageBuilder::ImageRecipe	Sí	Sí
AWS::ImageBuilder::InfrastructureConfiguration	Sí	Sí
AWS::InspectorV2::Activation	Sí	Sí
AWS::IoT::AccountAuditConfiguración	Sí	Sí
AWS::IoT::Authorizer	Sí	Sí
AWS::IoT:: CACertificate	Sí	Sí
AWS::IoT::CustomMetric	Sí	Sí
AWS::IoT::Dimension	Sí	Sí
AWS::IoT::FleetMetric	Sí	Sí
AWS::IoT::JobTemplate	Sí	Sí
AWS::IoT::MitigationAction	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::IoT::Policy	Sí	Sí
AWS::IoT::ProvisioningTemplate	Sí	Sí
AWS::IoT::RoleAlias	Sí	Sí
AWS::IoT::ScheduledAudit	Sí	Sí
AWS::IoT::SecurityProfile	Sí	Sí
AWS::IoT::ThingGroup	Sí	Sí
AWS::IoTEvents::AlarmModel	Sí	No
AWS::IoTEvents::DetectorModel	Sí	No
AWS::IoTEvents::Input	Sí	No
AWS::IoTSiteWise::Asset	Sí	No
AWS::IoTSiteWise::AssetModel	Sí	No
AWS::IoTSiteWise::Gateway	Sí	No

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::IoTSiteWise::Portal	Sí	No
AWS::IoTTwinMaker::ComponentType	Sí	No
AWS::IoTTwinMaker::Entity	Sí	No
AWS::IoTTwinMaker::Workspace	Sí	No
AWS::KMS::Alias	Sí	Sí
AWS::KMS::Key	Sí	Sí
AWS::Kinesis::Stream	Sí	Sí
AWS::Kinesis::StreamConsumer	Sí	Sí
AWS::KinesisAnalyticsV2::Application	Sí	Sí
AWS::KinesisFirehose::DeliveryStream	Sí	Sí
AWS::Lambda::Function	Sí	Sí
AWS::Location::GeofenceCollection	Sí	No

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::Location::Map	Sí	No
AWS::Location::PlaceIndex	Sí	No
AWS::Location::RouteCalculator	Sí	No
AWS::Logs::Destination	Sí	Sí
AWS::MSK::BatchScramSecreto	Sí	Sí
AWS::MSK::Cluster	Sí	Sí
AWS::MSK::ClusterPolicy	Sí	Sí
AWS::MSK::Configuration	Sí	Sí
AWS::MSK::VpcConnection	Sí	Sí
AWS::NetworkFirewall::Firewall	Sí	Sí
AWS::NetworkFirewall::FirewallPolicy	Sí	Sí
AWS::NetworkFirewall::RuleGroup	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::NetworkFirewall::VpcEndpointAsociación	Sí	Sí
AWS::NetworkManager::CustomerGatewayAsociación	Sí	No
AWS::NetworkManager::Device	Sí	No
AWS::NetworkManager::GlobalNetwork	Sí	No
AWS::NetworkManager::Link	Sí	No
AWS::NetworkManager::LinkAssociation	Sí	No
AWS::NetworkManager::Site	Sí	No
AWS::NetworkManager::TransitGatewayInscripción	Sí	No
AWS::OpenSearch::Domain	Sí	Sí
AWS::OpenSearchServerless::SecurityConfig	Sí	Sí
AWS::Pinpoint::App	Sí	No
AWS::Pinpoint::ApplicationSettings	Sí	No

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::Pinpoint::Campaign	Sí	No
AWS::Pinpoint::EmailChannel	Sí	No
AWS::Pinpoint::EmailTemplate	Sí	No
AWS::Pinpoint::EventStream	Sí	No
AWS::Pinpoint::InAppPlantilla	Sí	No
AWS::Pinpoint::Segment	Sí	No
AWS::QuickSight::Dashboard	Sí	Sí
AWS::QuickSight::Template	Sí	No
AWS: :RDS: DBCluster	Sí	Sí
AWS: :RDS:: Instantánea DBCluster	Sí	Sí
AWS: :RDS: DBInstance	Sí	Sí
AWS: :RDS:: Punto final DBProxy	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS: :RDS:: Grupo DBSecurity	Sí	Sí
AWS: :RDS: DBSnapshot	Sí	Sí
AWS: :RDS:: Grupo DBSubnet	Sí	Sí
AWS::RDS::EventSubscription	Sí	Sí
AWS::RDS::OptionGroup	Sí	Sí
AWS::Redshift::Cluster	Sí	Sí
AWS::Redshift::ClusterParameterGrupo	Sí	Sí
AWS::Redshift::ClusterSecurityGrupo	Sí	Sí
AWS::Redshift::ClusterSnapshot	Sí	Sí
AWS::Redshift::ClusterSubnetGrupo	Sí	Sí
AWS::Redshift::EventSubscription	Sí	Sí
AWS::Redshift::Integration	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::Redshift::ScheduledAction	Sí	Sí
AWS::RoboMaker::RobotApplication	Sí	No
AWS::RoboMaker::RobotApplicationVersión	Sí	No
AWS::RoboMaker::SimulationApplication	Sí	No
AWS::RolesEn cualquier lugar: :CRL	Sí	Sí
AWS::RolesAnywhere::Profile	Sí	Sí
AWS::RolesAnywhere::TrustAnchor	Sí	Sí
AWS::Route53Profiles::Profile	Sí	Sí
AWS::Route53Profiles::ProfileAssociation	Sí	Sí
AWS::Route53Resolver::FirewallDomainLista	Sí	Sí
AWS::Route53Resolver::FirewallRuleGrupo	Sí	Sí
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::Route53Resolver::ResolverEndpoint	Sí	Sí
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sí	Sí
AWS::Route53Resolver::Resol verQueryLoggingConfigAssociation	Sí	Sí
AWS::Route53Resolver::ResolverRule	Sí	Sí
AWS::Route53Resolver::ResolverRuleAsociación	Sí	Sí
AWS::S3::AccessGrant	Sí	Sí
AWS::S3::AccessGrantsInstancia	Sí	Sí
AWS::S3::AccessGrantsLocation	Sí	Sí
AWS::S3::AccessPoint	Sí	Sí
AWS::S3::AccountPublicAccessBlock	Sí	Sí
AWS::S3::Bucket	Sí	Sí
AWS::SES::ConfigurationSet	Sí	No

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::SES::ContactList	Sí	No
AWS::SES::DedicatedIpPiscina	Sí	Sí
AWS::SES::Template	Sí	No
AWS::SNS::Topic	Sí	Sí
AWS::SQS::Queue	Sí	Sí
AWS::SSM::AssociationCompliance	Sí	Sí
AWS::SSM::Document	Sí	Sí
AWS::SSM::FileData	Sí	Sí
Inventario de AWS::SSM::ManagedInstance	Sí	Sí
AWS::SSM::PatchCompliance	Sí	Sí
AWS::SSM::ResourceDataSincronizar	Sí	Sí
AWS::SageMaker::Model	Sí	No

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::SageMaker::NotebookInstance	Sí	No
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sí	No
AWS::SageMaker::StudioLifecycleConfig	Sí	Sí
AWS::SageMaker::UserProfile	Sí	Sí
AWS::SecretsManager::ResourcePolicy	Sí	Sí
AWS::SecretsManager::RotationSchedule	Sí	Sí
AWS::SecretsManager::Secret	Sí	Sí
AWS::SecurityHub::Standard	Sí	Sí
AWS::ServiceCatalog::CloudFormationProducto	Sí	Sí
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sí	Sí
AWS::ServiceCatalog::Portfolio	Sí	Sí
AWS::ServiceDiscovery::HttpNamespace	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::ServiceDiscovery::Instance	Sí	Sí
AWS::ServiceDiscovery::Service	Sí	Sí
AWS::StepFunctions::StateMachine	Sí	Sí
AWS::Transfer::Agreement	Sí	Sí
AWS::Transfer::Certificate	Sí	Sí
AWS::Transfer::Connector	Sí	Sí
AWS::Transfer::Profile	Sí	Sí
AWS::Transfer::Server	Sí	Sí
AWS::Transfer::Workflow	Sí	Sí
AWS::WAFRegional::RateBasedRegla	Sí	Sí
AWS::WAFRegional::Rule	Sí	Sí
AWS::WAFRegional::RuleGroup	Sí	Sí

Tipo de recurso	AWS GovCloud (EE. UU.-Oeste)	AWS GovCloud (EE. UU.-Este)
AWS::WAFRegional::WebACL	Sí	Sí
AWS:WAFv2:: IPSet	Sí	Sí
AWS::WAFv2::ManagedRuleSet	Sí	Sí
AWS::WAFv2::RegexPatternSet	Sí	Sí
AWS::WAFv2::RuleGroup	Sí	Sí
AWS::WAFv2::WebACL	Sí	Sí
AWS::WorkSpaces::Workspace	Sí	No

Grabación de AWS recursos con AWS Config

AWS Config detecta continuamente cuándo se crean, modifican o eliminan los tipos de recursos compatibles. AWS Config registra estos eventos como elementos de configuración (CIs).

Puede personalizarlos AWS Config para registrar los cambios de configuración de todos los tipos de recursos compatibles o solo de los tipos de recursos compatibles que sean relevantes para usted. Para obtener una lista de los tipos de recursos compatibles que AWS Config se pueden registrar, consulte Tipos de recursos compatibles para AWS Config.

Temas

- Consideraciones
- ¿En qué se diferencian los recursos regionales y globales?

- AWS Config Reglas y tipos de recursos globales
- Frecuencia de grabación para AWS Config
- Recursos no registrados
- Recursos de grabación en la AWS Config consola
- Grabación de recursos con la AWS CLI
- Excluir recursos de la grabación con AWS Config
- Dejar AWS Config de grabar con el grabador de configuración gestionado por el cliente

Consideraciones

Número elevado de AWS Config evaluaciones

Es posible que notes un aumento de la actividad en tu cuenta durante el primer mes de grabación con AWS Config en comparación con los meses siguientes. Durante el proceso de arranque inicial, AWS Config realiza evaluaciones de todos los recursos de tu cuenta que hayas seleccionado para AWS Config registrarlos.

Si ejecuta cargas de trabajo efímeras, es posible que vea un aumento de la actividad debido a que registra los cambios de AWS Config configuración asociados con la creación y la eliminación de estos recursos temporales. Una carga de trabajo efímera es el uso temporal de recursos informáticos que se cargan y ejecutan cuando es necesario. Los ejemplos incluyen instancias de spot de Amazon Elastic Compute Cloud (Amazon EC2), trabajos de Amazon EMR y AWS Auto Scaling.

Si quiere evitar el aumento de actividad derivado de la ejecución de cargas de trabajo efímeras, puede configurar el registrador de configuración gestionado por el cliente para que no se registren estos tipos de recursos, o bien ejecutar estos tipos de cargas de trabajo en una cuenta independiente y AWS Config desactivarla para evitar aumentar el registro de la configuración y la evaluación de las reglas.

Disponibilidad por región

Antes de especificar el tipo de recurso del que se va AWS Config a realizar el seguimiento, compruebe la disponibilidad de la cobertura de los recursos por región para comprobar si el tipo de recurso es compatible con la AWS región en la que lo configuró. AWS Config

Si al menos una región admite un tipo de recurso, puede habilitar el registro de ese tipo de recurso en todas las regiones admitidas AWS Config, incluso si el tipo de recurso especificado no es compatible con la AWS región en la que lo configuró AWS Config. AWS Config

¿En qué se diferencian los recursos regionales y globales?

Recursos regionales

Los recursos regionales están vinculados a una región y solo se pueden utilizar en esa región. Los crea en una región específica y Región de AWS, después, existen en esa región. Para ver esos recursos o interactuar con ellos, debe dirigir sus operaciones hacia esa región. Por ejemplo, para crear una instancia de Amazon EC2 con Consola de administración de AWS, elige la instancia en la Región de AWS que desea crear la instancia. Si usa AWS Command Line Interface (AWS CLI) para crear la instancia, incluye el `--region` parámetro. AWS SDKs Cada uno tiene su propio mecanismo equivalente para especificar la región que utiliza la operación.

Existen varios motivos para utilizar los recursos regionales. Una razón es asegurarse de que los recursos y los puntos de conexión de servicio que se utilizan para acceder a ellos estén lo más cerca posible del cliente. Esto mejora el rendimiento al minimizar la latencia. Otra razón es proporcionar un límite de aislamiento. Esto permite crear copias independientes de los recursos en varias regiones para distribuir la carga y mejorar la escalabilidad. Al mismo tiempo, aísla los recursos unos de otros para mejorar la disponibilidad.

Si especificas otro Región de AWS en la consola o en un AWS CLI comando, ya no podrás ver ni interactuar con los recursos que veías en la región anterior.

Cuando consulta el nombre de recurso de Amazon (ARN) de un recurso regional, la región que contiene el recurso se especifica como el cuarto campo del ARN. Por ejemplo, una instancia de Amazon EC2 es un recurso regional. A continuación, se muestra un ejemplo de un ARN para una instancia de Amazon EC2 en la región de `us-east-1`.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Recursos globales

Algunos recursos de AWS servicios son recursos globales, lo que significa que puede utilizar el recurso desde cualquier lugar. No se especifica ninguna Región de AWS en la consola de un servicio global. Para acceder a un recurso global, no se especifica ningún `--region` parámetro al utilizar las operaciones del servicio AWS CLI y del AWS SDK.

Los recursos globales admiten casos en los que es fundamental que solo pueda existir una instancia de un recurso concreto a la vez. En estos escenarios, la replicación o la sincronización entre copias en diferentes regiones no son adecuadas. Tener que acceder a un único punto de

conexión global, con el posible aumento de la latencia, se considera aceptable para garantizar que cualquier cambio sea visible de forma instantánea para los consumidores del recurso.

Por ejemplo, los clústeres globales de Amazon Aurora (`AWS::RDS::GlobalCluster`) son recursos globales y, por lo tanto, no están vinculados a una región. Esto significa que puede crear un clúster global sin depender de un punto de conexión regional. La ventaja es que, si bien el propio Amazon Relational Database Service (Amazon RDS) está organizado por regiones, la región específica en la que se origina un clúster global no afecta al clúster global. Aparece como un clúster global único y continuo en todas las regiones.

El nombre de recurso de Amazon (ARN) de un recurso global no incluye una región. El cuarto campo está vacío, como en el siguiente ejemplo de un ARN para un clúster global.

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> Los tipos de recursos globales incorporados AWS Config después de febrero de 2022 solo se registrarán en la región de origen del servicio en el caso de la partición comercial y AWS GovCloud (EE. UU. al oeste) en el caso de la partición. GovCloud Puede ver los elementos de configuración (CIs) de estos nuevos tipos de recursos globales solo en su región de origen y AWS GovCloud (EE. UU. al oeste).
> Los tipos de recursos globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role` y`AWS::IAM::User`) permanecen sin cambios. Puede habilitar el registro de estos recursos de IAM globales en todas las regiones en las que AWS Config se admitía antes de febrero de 2022. Estos recursos de IAM globales no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022.

Tipos de recursos globales | Recursos de IAM

Los siguientes tipos de recursos de IAM son recursos globales: usuarios, grupos, roles y políticas administradas por el cliente de IAM. Estos tipos de recursos se pueden registrar AWS Config en las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Esta lista incluye las regiones donde no puede registrar los tipos de registros de IAM globales: Asia-Pacífico (Hyderabad), Asia-Pacífico (Malasia) Asia-Pacífico (Melbourne), Asia-Pacífico

(Tailandia), Oeste de Canadá (Calgary) Europa (España), Europa (Zúrich), Israel (Tel Aviv), México (centro) y Medio Oriente (EAU).

Para evitar la duplicación de los elementos de configuración (CIs), debería considerar registrar solo los tipos de recursos de IAM globales una vez en una de las regiones compatibles. Esto también puede ayudarle a evitar las evaluaciones innecesarias y la limitación de las API.

Tipos de recursos globales | Solo en la región de origen

Los recursos globales para los siguientes servicios solo se registran AWS Config en la región de origen del tipo de recurso global: Amazon Elastic Container Registry Public AWS Global Accelerator, Amazon Route 53 CloudFront, Amazon y AWS WAF. Para estos recursos globales, se puede usar la misma instancia del tipo de recurso en varias AWS regiones, pero los elementos de configuración (CIs) solo se registran en la región de origen de la partición comercial o AWS GovCloud (EE. UU. al oeste) para la AWS GovCloud (US) partición.

Regiones de origen para los tipos de recurso globales

AWS Servicio	Valor de tipo de recurso	Región de origen
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	Región Este de EE. UU. (Norte de Virginia)
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	Región del Oeste de EE. UU (Oregón)
	`AWS::GlobalAccelerator::EndpointGroup`	Región del Oeste de EE. UU (Oregón)
	`AWS::GlobalAccelerator::Accelerator`	Región del Oeste de EE. UU (Oregón)
Amazon Route 53	`AWS::Route53::HostedZone`	Región Este de EE. UU. (Norte de Virginia)
	`AWS::Route53::HealthCheck`	Región Este de EE. UU. (Norte de Virginia)
Amazon CloudFront	`AWS::CloudFront::Distribution`	Región Este de EE. UU. (Norte de Virginia)

AWS Servicio	Valor de tipo de recurso	Región de origen
AWS WAF	`AWS::WAFv2::WebACL`	Región Este de EE. UU. (Norte de Virginia)

Tipos de recursos globales | clústeres globales de Aurora

`AWS::RDS::GlobalClusteres` un recurso global que se registra en todas AWS Config las regiones compatibles en las que está activado el registrador de configuración gestionado por el cliente. Este tipo de recurso global es único, ya que si habilita el registro de este recurso en una región, AWS Config registrará los elementos de configuración (CIs) de este tipo de recurso en todas las regiones habilitadas.

Si no desea registrar `AWS::RDS::GlobalCluster` en todas las regiones habilitadas, utilice una de las siguientes estrategias de registro para la consola de AWS Config :

- Registre todos los tipos de recursos con anulaciones personalizables, elija GlobalCluster «AWS RDS» y elija la anulación «Excluir de la grabación»
- Registrar los tipos de recurso específicos.

Si no desea registrar `AWS::RDS::GlobalCluster` en todas las regiones habilitadas, utilice una de las siguientes estrategias de registro para API/CLI:

- Registrar todos los tipos de recursos actuales y futuros con exclusiones (`EXCLUSION_BY_RESOURCE_TYPES`)
- Registrar los tipos de recursos específicos (`INCLUSION_BY_RESOURCE_TYPES`).

AWS Config Reglas y tipos de recursos globales

Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos de IAM globales no se pueden registrar en las regiones admitidas después de febrero de AWS Config 2022. Para obtener una lista de esas regiones, consulte Recording AWS Resources | Global Resources.

Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas

las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.

Prácticas recomendadas para informar sobre el cumplimiento de los recursos globales incorporados antes de febrero de 2022

Para evitar evaluaciones innecesarias, solo debes implementar AWS Config reglas y paquetes de conformidad que incluyan estos recursos globales en una de las regiones compatibles. Para saber qué reglas administradas son compatibles en cada región, consulte la lista List of AWS Config Managed Rules by Region Availability. Esto se aplica a AWS Config las reglas, a AWS Config las reglas organizativas y también a las reglas creadas por otros AWS servicios, como AWS Security Hub CSPM y AWS Control Tower.

Si no va a registrar los tipos de recursos globales incorporados antes de febrero de 2022, se recomienda no activar las siguientes reglas periódicas para evitar evaluaciones innecesarias:

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- mfa-enabled-for-iam-acceso a la consola
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled

Prácticas recomendadas para informar sobre el cumplimiento de los recursos globales incorporados después de febrero de 2022

Los tipos de recursos globales incorporados a la AWS Config grabación después de febrero de 2022 solo se registrarán en la región de origen del servicio en el caso de la partición comercial y AWS GovCloud (EE. UU. al oeste) en el caso de la partición. AWS GovCloud (US) Debe implementar AWS Config reglas y paquetes de conformidad que incluyan estos recursos globales solo en la región de origen del tipo de recurso. Para obtener más información, consulte Home Regions for Global Resource Types.

Frecuencia de grabación para AWS Config

AWS Config admite la grabación continua y la grabación diaria. El registro continuo permite registrar los cambios de configuración de forma continua siempre que se produzca un cambio. El registro diario permite recibir un elemento de configuración (CI) que representa el estado más reciente de los recursos durante el último período de 24 horas, solo si es diferente del CI anterior registrado. Si desea saber cuáles son los pasos para cambiar la frecuencia de grabación, consulte Changing Recording Frequency.

Registro continuo

Algunos de los beneficios del registro continuo son:

- Supervisión en tiempo real: el registro continuo puede proporcionar una detección inmediata de cambios no autorizados o alteraciones inesperadas, lo que puede mejorar sus esfuerzos de seguridad y cumplimiento.
- Análisis detallado: el registro continuo le permite analizar en profundidad los cambios de configuración de sus recursos a medida que se producen, lo que le permite identificar patrones y tendencias en cualquier momento.

Registro diario

Algunos de los beneficios del registro diario son:

- Interrupción mínima: el registro diario puede proporcionarle un flujo de información más manejable, lo que puede reducir la frecuencia de las notificaciones y la fatiga de las alertas.
- Rentabilidad: el registro diario puede proporcionarle la flexibilidad de registrar los cambios en sus recursos con una frecuencia menor, lo que puede reducir los costes relacionados con la cantidad de cambios de configuración registrados.

> **Note**
>
> AWS Firewall Manager depende de la grabación continua para monitorear sus recursos. Si utiliza Firewall Manager, se recomienda configurar la frecuencia de registro en Continua.

Recursos no registrados

Si un recurso no está registrado, AWS Config captura únicamente la creación y eliminación de ese recurso, sin ningún otro detalle, sin coste alguno para usted. Cuando se crea o elimina un recurso no registrado, AWS Config envía una notificación y muestra el evento en la página de detalles del recurso. La página de detalles de un recurso no registrado proporciona valores nulos para la mayoría de los detalles de la configuración y no proporciona información acerca de las relaciones y los cambios de configuración.

La información de relación que se AWS Config proporciona para los recursos registrados no está limitada debido a la falta de datos en los recursos no registrados. Si un recurso registrado está relacionado con un recurso no registrado, esa relación se proporciona en la página de detalles del recurso registrado.

Consideraciones sobre los tipos de recursos de IAM

Los tipos de recurso `AWS::IAM::User`, `AWS::IAM::Policy`, `AWS::IAM::Group` y `AWS::IAM::Role` solo capturarán los estados de creación (`ResourceNotRecorded`) y eliminación (`ResourceDeletedNotRecorded`) si el recurso está seleccionado (o si se seleccionó anteriormente) como recurso para registrarlo en el registrador de configuración administrado por el cliente.

Programación de registro de CI de recursos no registrados

Los elementos de configuración (CIs) para `ResourceNotRecorded` y `ResourceDeletedNotRecorded` no siguen el tiempo de registro típico para los tipos de recursos. Estos tipos de recursos solo se registran durante el proceso periódico de línea de base del registrador de configuración administrado por el cliente, que tiene un ritmo menos frecuente que el de los demás tipos de recursos. Esto significa que las notificaciones de creación y eliminación no se envían al crearlas o eliminarlas, sino durante el proceso de establecimiento de la línea de base.

Ámbito de la entrega de CI y del registrador vinculado a servicios

En el caso de los grabadores de configuración vinculados a servicios, el alcance del registro determina si recibe los elementos de configuración (CIs) en el canal de entrega. El ámbito de registro lo establece el servicio que está vinculado al registrador de configuración. Si el ámbito de grabación es interno, no los recibirá CIs en el canal de entrega.

Recursos de grabación en la AWS Config consola

Puede utilizar la AWS Config consola para seleccionar los tipos de recursos que se AWS Config registran en el grabador de configuración gestionado por el cliente.

Para seleccionar recursos

1. Inicie sesión en la AWS Config consola Consola de administración de AWS y ábrala desde https://console.aws.amazon.com/config/casa.
2. Elija Configuración en el panel de navegación izquierdo.
3. En la pestaña Registrador administrado por el cliente, seleccione Editar.
4. En la sección Método de grabación, elija una estrategia de registro. Puede especificar los AWS recursos que AWS Config desea grabar.

   All resource types with customizable overrides

   Se configura AWS Config para registrar los cambios de configuración de todos los tipos de recursos compatibles actuales y futuros en esta región. Puede anular la frecuencia de registro para tipos de recursos específicos o excluir tipos de recursos específicos del registro. Para obtener más información, consulte Tipos de recursos admitidos.

   - Configuración predeterminada

     Configure la frecuencia de registro predeterminada para todos los tipos de recursos compatibles actuales y futuros. Para obtener más información, consulte Frecuencia de registro.

     - Grabación continua: AWS Config registrará los cambios de configuración de forma continua siempre que se produzca un cambio.
     - Registro diario: recibirá un elemento de configuración (CI) que representa el estado más reciente de sus recursos durante el último período de 24 horas, solo si es diferente del CI anterior registrado.

     > **Note**
     >
     > AWS Firewall Manager depende de la grabación continua para monitorear sus recursos. Si utiliza Firewall Manager, se recomienda configurar la frecuencia de registro en Continua.

- Anular la configuración

  Puede anular la frecuencia de registro para tipos de recursos específicos o excluir tipos de recursos específicos del registro. Si cambia la frecuencia de registro de un tipo de recurso, o deja de registrar un tipo de recurso, los elementos de configuración que ya estaban registrados permanecerán sin cambios.

Specific resource types

Se configura AWS Config para registrar los cambios de configuración únicamente para los tipos de recursos que especifique.

- Tipos de recurso específicos

  Elija un tipo de recurso que desee registrar y su frecuencia. Para obtener más información, consulte Frecuencia de registro.

  - Grabación continua: AWS Config registrará los cambios de configuración de forma continua siempre que se produzca un cambio.
  - Registro diario: recibirá un elemento de configuración (CI) que representa el estado más reciente de sus recursos durante el último período de 24 horas, solo si es diferente del CI anterior registrado.

  > **Note**
  >
  > AWS Firewall Manager depende de la grabación continua para monitorear sus recursos. Si utiliza Firewall Manager, se recomienda configurar la frecuencia de registro en Continua.

  Si cambia la frecuencia de registro de un tipo de recurso, o deja de registrar un tipo de recurso, los elementos de configuración que ya estaban registrados permanecerán sin cambios.

5. Elija Guardar para guardar los cambios.

Consideraciones al registrar los recursos

Alto número de AWS Config evaluaciones

Es posible que notes un aumento de la actividad en tu cuenta durante el primer mes de grabación con AWS Config en comparación con los meses siguientes. Durante el proceso de arranque inicial, AWS Config realiza evaluaciones de todos los recursos de tu cuenta que hayas seleccionado para AWS Config registrarlos.

Si ejecuta cargas de trabajo efímeras, es posible que vea un aumento de la actividad debido a que registra los cambios de AWS Config configuración asociados con la creación y la eliminación de estos recursos temporales. Una carga de trabajo efímera es el uso temporal de recursos informáticos que se cargan y ejecutan cuando es necesario. Algunos ejemplos son las instancias puntuales de Amazon Elastic Compute Cloud (Amazon EC2), los trabajos de Amazon EMR y. AWS Auto Scaling Si quiere evitar el aumento de actividad derivado de la ejecución de cargas de trabajo efímeras, puede configurar el registrador de configuración administrado por el cliente para que no se registren estos tipos de recursos o ejecutar estos tipos de cargas de trabajo en una cuenta independiente con la opción AWS Config desactivada para evitar aumentar el registro de la configuración y las evaluaciones de las reglas.

Considerations: All resource types with customizable overrides

Tipos de recursos registrados de forma global | Los clústeres globales de Aurora se incluyen inicialmente en el registro

El tipo `AWS::RDS::GlobalCluster` de recurso se registrará en todas las AWS Config regiones compatibles en las que esté activado el registrador de configuración gestionado por el cliente.

Si no desea registrar `AWS::RDS::GlobalCluster` en todas las regiones habilitadas, elija «AWS RDS GlobalCluster» y «Excluir del registro».

Tipos de recursos globales | Los tipos de recursos de IAM se excluyen inicialmente del registro

Inicialmente, se excluyen del registro los tipos de recursos de IAM globales, para ayudarle a reducir los costos. Esta agrupación incluye usuarios, grupos, roles y políticas administradas por el cliente de de IAM. Seleccione Eliminar para eliminar la anulación e incluir estos recursos en el registro.

Además, los tipos de recursos de IAM globales (`AWS::IAM::User`, `AWS::IAM::GroupAWS::IAM::Role`, y`AWS::IAM::Policy`) no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para obtener una lista de esas regiones, consulte AWS Recursos de grabación | Recursos globales.

Límites

Puede añadir hasta 100 anulaciones de frecuencia y 600 anulaciones de exclusión.

No se admite la grabación diaria para los siguientes tipos de recursos:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

Disponibilidad por región

Antes de especificar el tipo de recurso AWS Config que deseas rastrear, comprueba la cobertura de recursos por región y disponibilidad para ver si el tipo de recurso es compatible con la AWS región en la que lo configuraste AWS Config. Si al menos una región admite un tipo de recurso, puede habilitar el registro de ese tipo de recurso en todas las regiones admitidas AWS Config, incluso si el tipo de recurso especificado no es compatible con la AWS región en la que lo configuró AWS Config. AWS Config

Límites

No hay límites si todos los tipos de recursos tienen la misma frecuencia. Puede agregar hasta 100 tipos de recursos con la frecuencia diaria si al menos un tipo de recursos está configurado como Continuo.

No se admite el registro diario para los siguientes tipos de recursos:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Grabación de recursos con la AWS CLI

Puede usar la AWS CLI para seleccionar los tipos de recursos que AWS Config desea registrar. Para ello, se crea un registrador de configuración, que registra los tipos de recursos que especifique en un grupo de registro. En el grupo de registro, debe especificar si quiere registrar todos los tipos de recurso admitidos o incluir o excluir determinados tipos de recursos.

Record all current and future supported resource types

Se configura AWS Config para registrar los cambios de configuración de todos los tipos de recursos compatibles actuales y futuros en esta región. Para obtener una lista de tipos de recursos compatibles, consulte Tipos de recursos compatibles.

1. Utilice el comando `put-configuration-recorder`:

   Este comando usa los campos `--configuration-recorder` y `---recording-group`.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

   El campo **`configuration-recorder`**

   El archivo `configurationRecorder.json` especifica el `name` y el `roleArn`, además de la frecuencia de registro predeterminada para el registro de la configuración (`recordingMode`).

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

   El campo **`recording-group`**

   El campo `recordingGroup.json` especifica los tipos de recursos que se registran.

```
{
```

```
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

Para obtener más información acerca de estos campos, consulte put-configuration-recorder en la Referencia de comandos de la AWS CLI .

2. (Opcional) Para verificar que el registrador de configuración administrado por el cliente tiene la configuración que desea, utilice el siguiente comando describe-configuration-recorders.

```
$ aws configservice describe-configuration-recorders
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
```

```
                ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

Se configura AWS Config para registrar los cambios de configuración de todos los tipos de recursos compatibles actuales y futuros, incluidos los tipos de recursos globales, excepto los tipos de recursos que especifique que se excluyan del registro.

Si decide dejar de registrar un tipo de recurso, los elementos de configuración que ya estaban registrados permanecerán sin cambios. Para obtener una lista de tipos de recursos compatibles, consulte Tipos de recursos compatibles.

1. Utilice el comando `put-configuration-recorder`:

   Este comando usa los campos `--configuration-recorder` y `---recording-group`.

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   El campo **`configuration-recorder`**

   El archivo `configurationRecorder.json` especifica el `name` y el `roleArn`, además de la frecuencia de registro predeterminada para el registro de la configuración (`recordingMode`).

   ```
   {
     "name": "default",
     "roleARN": "arn:aws:iam::123456789012:role/config-role",
     "recordingMode": {
       "recordingFrequency": CONTINUOUS or DAILY,
       "recordingModeOverrides": [
           {
               "description": "Description you provide for the override",
               "recordingFrequency": CONTINUOUS or DAILY,
               "resourceTypes": [ Comma-separated list of resource types to include
    in the override ]
   ```

```
        }
    ]
  }
}
```

El campo **`recording-group`**

El `recordingGroup.json` archivo especifica qué tipos de recursos AWS Config se registrarán. Pase uno o más tipos de recursos para excluir en el campo `resourceTypes` de `exclusionByResourceTypes`, tal y como se muestra en el siguiente ejemplo.

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

Para obtener más información acerca de estos campos, consulte `put-configuration-recorder` en la Referencia de comandos de la AWS CLI .

2. (Opcional) Para verificar que el registrador de configuración administrado por el cliente tiene la configuración que desea, utilice el siguiente comando `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "ConfigurationRecorders": [
        {
```

```
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

Se configura AWS Config para registrar los cambios de configuración únicamente para los tipos de recursos que especifique.

Si decide dejar de registrar un tipo de recurso, los elementos de configuración que ya estaban registrados permanecerán sin cambios. Para obtener una lista de tipos de recursos compatibles, consulte Tipos de recursos compatibles.

1. Utilice el comando `put-configuration-recorder`:

Este comando usa los campos `--configuration-recorder` y `---recording-group`.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

El campo **`configuration-recorder`**

El archivo `configurationRecorder.json` especifica el `name` y el `roleArn`, además de la frecuencia de registro predeterminada para el registro de la configuración (`recordingMode`).

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

El campo **`recording-group`**

El `recordingGroup.json` archivo especifica qué tipos de recursos AWS Config se registrarán. Pase uno o más tipos de recursos para excluir en el campo `resourceTypes`, tal y como se muestra en el siguiente ejemplo.

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
```

```
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

Para obtener más información acerca de estos campos, consulte `put-configuration-recorder` en la Referencia de comandos de la AWS CLI .

2. (Opcional) Para verificar que el registrador de configuración administrado por el cliente tiene la configuración que desea, utilice el siguiente comando `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
```

```
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Excluir recursos de la grabación con AWS Config

AWS Config le permite excluir tipos específicos de AWS recursos del seguimiento del inventario y la supervisión del cumplimiento y, al mismo tiempo, realizar un seguimiento de todos los demás tipos de recursos compatibles disponibles actualmente AWS Config, incluidos los que se añadirán en el futuro. Puede usar esta característica para concentrarse en los recursos críticos que están sujetos a los estándares de cumplimiento y gobernanza.

Excluding resources (Console)

Si no desea grabar un tipo de AWS recurso, utilice una de las siguientes estrategias de grabación para la AWS Config consola:

- Registrar todos los tipos de recursos con anulaciones personalizables: elija el tipo de recurso que desee excluir y elija la opción de anulación “Excluir del registro”.
- Registrar los tipos de recurso específicos.

Para ver los pasos más detallados, consulte Registro de recursos (consola).

Excluding resources (AWS CLI)

Si no desea grabar un tipo de AWS recurso, utilice una de las siguientes estrategias de grabación para la API/CLI:

- Registrar todos los tipos de recursos actuales y futuros con exclusiones (`EXCLUSION_BY_RESOURCE_TYPES`)
- Registrar los tipos de recursos específicos (`INCLUSION_BY_RESOURCE_TYPES`).

Para ver los pasos más detallados, consulte Recording Resources (AWS CLI).

Dejar AWS Config de grabar con el grabador de configuración gestionado por el cliente

Puede dejar AWS Config de grabar en cualquier momento con el grabador de configuración gestionado por el cliente. Cuando AWS Config deja de grabar un recurso, conserva la información de configuración que se capturó anteriormente y usted puede seguir accediendo a esta información.

Si desea ver los pasos para detener el registro, consulte Detención del registrador de configuración administrado por el cliente.

Grabación de configuraciones con AWS Config recursos de terceros mediante AWS CLI

Registre las configuraciones de recursos de terceros o tipos de recursos personalizados, como servidores locales, herramientas de monitoreo de SAAS y sistemas de control de versiones (por ejemplo GitHub).

Puede publicar los datos de configuración de recursos de terceros AWS Config y ver y supervisar el inventario de recursos y el historial de configuración mediante la AWS Config consola y APIs. Puede utilizarlos AWS Config para administrar todos sus recursos y evaluar la configuración de los recursos para comprobar si cumplen con las mejores prácticas de uso de AWS Config reglas. También puede crear AWS Config reglas o paquetes de conformidad para evaluar estos recursos de terceros comparándolos con las mejores prácticas, las políticas internas y las políticas reglamentarias.

> **Note**
>
> Si lo ha configurado AWS Config para registrar todos los tipos de recursos, los recursos de terceros que se administran (crean, actualizan o eliminan) a través de ellos CloudFormation se registran automáticamente AWS Config como elementos de configuración.

Requisito previo: los recursos de terceros o el tipo de recurso personalizado deben registrarse utilizando CloudFormation.

Temas

- Añadir recursos de terceros a AWS Config
- Registre los elementos de configuración con AWS Config recursos de terceros mediante el AWS CLI
- Lea los elementos de configuración con AWS Config recursos de terceros mediante el AWS CLI
- Elimine los recursos de terceros para que no AWS Config utilicen la AWS CLI

Añadir recursos de terceros a AWS Config

Siga estos pasos para añadir un recurso de terceros a AWS Config.

Temas

- Paso 1: Configure el entorno de desarrollo
- Paso 2: Modele su recurso
- Paso 3: Genere artefactos
- Paso 4: Registre el recurso
- Paso 5: Publique la configuración del recurso

Paso 1: Configure el entorno de desarrollo

Instalar y configurar la CloudFormation AWS CLI. AWS CLI Le permite modelar y registrar sus recursos personalizados. Para obtener más información, consulte Recursos personalizados y ¿Qué es la interfaz de línea de CloudFormation comandos? .

Paso 2: Modele su recurso

Cree un esquema de proveedor de recursos que cumpla y valide la configuración del tipo de recurso.

1. Utilice el comando `init` para crear el proyecto de proveedor de recursos y generar los archivos necesarios.

```
$ cfn init
Initializing new project
```

2. El comando `init` inicia un asistente que le guía por la configuración del proyecto, incluida la especificación del nombre del recurso. En este tutorial, especifique `MyCustomNamespace::Testing::WordPress`.

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. Especifique el nombre de paquete del recurso.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> Para garantizar que cualquier dependencia del proyecto se resuelva correctamente, puede importar el proyecto generado a su IDE con ayuda de Maven.
> Por ejemplo, si utiliza el esquema IntelliJ IDEA, debe hacer lo siguiente:
>
> - En el menú Archivo, elija Nuevo y, a continuación, Proyecto de orígenes existentes.
> - Navegue hasta el directorio del proyecto.
> - En el cuadro de diálogo Importar proyecto, elija Importar proyecto desde un modelo externo y, a continuación, elija Maven.
> - Seleccione Siguiente y acepte los valores predeterminados para completar la importación del proyecto.

4. Abra el archivo `mycustomnamespace-testing-wordpress.json` que contiene el esquema del recurso. Copie y pegue el siguiente esquema en `mycustomnamespace-testing-wordpress.json`.

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. Valide el esquema.

```
$ cfn validate
```

6. Actualice los archivos generados automáticamente en el paquete del proveedor de recursos para ver las actualizaciones del esquema del proveedor de recursos. Al iniciar el proyecto del proveedor de recursos, AWS CLI genera los archivos y el código de apoyo para el proveedor de recursos. Vuelva a generar el código para ver el esquema actualizado.

```
$ cfn generate
```

> **Note**
>
> Al usar Maven, el comando `generate` se ejecuta automáticamente antes de compilar el código como parte del proceso de compilación. Por lo tanto, sus cambios nunca se desincronizarán con el código generado.
> Tenga en cuenta que la CloudFormation CLI debe estar en una ubicación que Maven/the el sistema pueda encontrar. Para obtener más información, consulte Setting up your environment for developing extensions.

Para obtener más información sobre todo el proceso, consulte Modeling Resource Providers for Use in CloudFormation.

Paso 3: Genere artefactos

Ejecute el siguiente comando para generar artefactos para `cfn submit`.

```
$ mvn package
```

Paso 4: Registre el recurso

AWS Config no requiere que los controladores del proveedor de recursos realicen el seguimiento de la configuración del recurso. Ejecute el siguiente comando para registrar el recurso.

```
$ cfn submit
```

Para obtener más información, consulte Registrar proveedores de recursos para su uso en CloudFormation plantillas.

Paso 5: Publique la configuración del recurso

Determine la configuración de MyCustomNamespace: :Testing::WordPress.

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
```

```
  "PublicIp": "my-wordpress-site.com"
}
```

Determine el identificador de versión del esquema desde CloudFormation `DescribeType`.

En AWS Config, puede ver si se acepta esta configuración de recursos. Para evaluar el cumplimiento, puede escribir AWS Config reglas con este recurso.

(Opcional) Para automatizar el registro de la configuración, implemente recopiladores de configuración periódicos o basados en cambios.

Registre los elementos de configuración con AWS Config recursos de terceros mediante el AWS CLI

Registre un elemento de configuración de un recurso de terceros o un tipo de recurso personalizado mediante el procedimiento que se muestra a continuación:

No olvide registrar el tipo de recurso `MyCustomNamespace::Testing::WordPress` con su esquema correspondiente.

1. Abra un símbolo del sistema o una ventana de terminal.
2. Introduzca el siguiente comando:

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> Tal como se define en el esquema de tipos, se `writeOnlyProperties` eliminará de la configuración antes de que se registre AWS Config. Esto significa que estos valores no estarán presentes cuando la configuración se obtenga de la lectura APIs. Para obtener más información sobre `writeOnlyProperties`, consulte Resource type schema.

Lea los elementos de configuración con AWS Config recursos de terceros mediante el AWS CLI

Lea un elemento de configuración de un recurso de terceros o un tipo de recurso personalizado mediante el procedimiento que se muestra a continuación:

1. Abra un símbolo del sistema o una ventana de terminal.
2. Introduzca el siguiente comando:

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. Pulse Intro.

   Debería ver una salida similar a esta:

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. Introduzca el siguiente comando:

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Pulse Intro.

   Debería ver una salida similar a esta:

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
```

```
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

Elimine los recursos de terceros para que no AWS Config utilicen la AWS CLI

Para eliminar un recurso de terceros, introduzca siguiente comando:

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

Si se ejecuta correctamente, el comando no muestra ninguna salida adicional.

Configuración del software de grabación para instancias administradas con AWS Config

Puede utilizarlo AWS Config para registrar los cambios en el inventario de software en las instancias de Amazon EC2 y en los servidores locales. De este modo, puede ver los cambios históricos en la configuración del software. Por ejemplo, cuando se instala una nueva actualización de Windows en una instancia de Windows administrada, AWS Config registra los cambios y, a continuación, los envía a su canal de entrega para que se le notifique sobre el cambio. Con AWS Config ella, puede ver el historial de cuándo se instalaron las actualizaciones de Windows para la instancia administrada y cómo cambiaron a lo largo del tiempo.

Temas

- Requisitos previos
- Registro de configuraciones de software

Requisitos previos

Debe realizar los siguientes pasos para registrar los cambios de configuración de software:

- Active el registro del tipo de recurso de inventario de la instancia administrada en AWS Config.
- Configure los servidores EC2 y locales como instancias administradas en. AWS Systems Manager Una instancia administrada es una máquina que ha sido configurada para usarse con Systems Manager.
- Inicie la recopilación del inventario de software de las instancias administradas mediante la capacidad de inventario de Systems Manager.

> **Note**
>
> Systems Manager ahora admite la creación de elementos de configuración para instancias no administradas
> El elemento de configuración para las instancias no administradas tendrá una configuración adicional con `Key: “InstanceStatus”` y `Value: “Unmanaged”`.
> Los elementos de configuración de las instancias no administradas no recibirán actualizaciones adicionales
> Para recibir actualizaciones adicionales, el elemento de configuración debe ser una instancia administrada.

También puede usar AWS Config las reglas para monitorear los cambios en la configuración del software y recibir notificaciones sobre si los cambios cumplen o no con sus reglas. Por ejemplo, si crea una regla que comprueba si sus instancias administradas tienen una aplicación concreta y una instancia no tiene instalada esa aplicación, AWS Config señala dicha instancia como no conforme con la regla. Para obtener una lista de las reglas AWS Config administradas, consulteLista de reglas AWS Config administradas.

Registro de configuraciones de software

Para habilitar el registro de los cambios de configuración del software en AWS Config:

1. Active el registro de todos los tipos de recursos admitidos, o bien registre de forma selectiva el tipo de recurso de inventario de instancia administrada en AWS Config. Para obtener más información, consulte Grabación de AWS recursos con AWS Config.

2. Lance una instancia de Amazon EC2 con un perfil de instancia para Systems Manager que incluya la política SSMManaged InstanceCore gestionada por Amazon. Esta política administrada por AWS permite que una instancia utilice la funcionalidad básica del servicio Systems Manager.

   Para obtener más información acerca de otras políticas que puede agregar al perfil de instancia de Systems Manager, consulte Creación de un perfil de instancias de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager .

   > **Important**
   >
   > El agente de SSM es software de Amazon que debe estar instalado en una instancia administrada para comunicarse con Systems Manager en la nube. Si la instancia EC2 se creó a partir de una AMI para uno de los siguientes sistemas operativos, el agente está preinstalado:
   >
   > - Windows Server 2003-2012 R2 AMIs publicado en noviembre de 2016 o después
   > - Windows Server 2016 y 2019
   > - Amazon Linux
   > - Amazon Linux 2
   > - Ubuntu Server 16.04
   > - Ubuntu Server 18.04
   >
   > En las instancias EC2 que no se crearon a partir de una AMI con el agente preinstalado, debe instalar el agente de forma manual. Para obtener información, consulte los siguientes temas en la Guía del usuario de AWS Systems Manager :
   >
   > - Instalación y configuración del agente de SSM en instancias EC2 para Windows Server
   > - Instalación y configuración del agente de SSM en instancias EC2 para Linux

3. Inicie una recopilación de inventario tal y como se describe en la sección Configuración de la recopilación de inventario en la Guía del usuario de AWS Systems Manager . Los procedimientos son los mismos para instancias de Linux y Windows.

   AWS Config puede registrar los cambios de configuración de los siguientes tipos de inventario:

- Aplicaciones: una lista de aplicaciones para instancias administradas, como software antivirus.
- AWS componentes: una lista de AWS componentes para las instancias administradas, como AWS CLI y SDKs.
- Información sobre instancias: información sobre instancias, como nombre y versión de SO, dominio y estado de firewall.
- Configuración de red: información de configuración, como dirección IP, puerta de enlace y máscara de subred.
- Actualizaciones de Windows: una lista de las actualizaciones de Windows de las instancias administradas (solo instancias de Windows).

> **Note**
>
> AWS Config no admite el registro del tipo de inventario personalizado en este momento.

La recopilación de inventario es una de las muchas capacidades de Systems Manager, que se agrupan en las categorías Administración de operaciones, Acciones y cambiar, Instancias y nodos y Recursos compartidos. Para obtener más información, consulte ¿Qué es Systems Manager? y Capacidades de Systems Manager en la Guía del usuario de AWS Systems Manager .

Búsqueda de recursos descubiertos por AWS Config

Puede usar la AWS Config consola y la AWS Config API para buscar los recursos que han AWS Config realizado un inventario o descubierto, incluidos los recursos eliminados y los recursos que no AWS Config se están grabando actualmente. AWS CLI AWS Config descubre únicamente los tipos de recursos compatibles. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.

Looking Up Resources (Console)

Puede utilizar tipos de recursos o información de etiquetas para buscar recursos en la consola de AWS Config .

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.

2. En la página Inventario de recursos, especifique las opciones de búsqueda de los recursos que desea buscar:
   - Categoría de recursos: elija todas las categorías de recursos o limite los resultados a solo AWS recursos.
   - Tipo de recurso: elija todos los tipos de recursos o seleccione los recursos por los que desee filtrar.
   - Cumplimiento: elija filtrar por cualquier estado de cumplimiento, conforme o no.
3. AWS Config muestra los recursos que coinciden con sus opciones de búsqueda. Puede consultar la siguiente información sobre los recursos:
   - Identificador de recursos: el identificador de recursos puede ser un ID de recurso o un nombre de recurso, si procede. Elija el enlace del identificador de recursos para ver la página de detalles de recursos.
   - Tipo de recurso: el tipo del recurso aparece en la lista.
   - Conformidad: el estado del recurso que AWS Config se evaluó según la regla.

Looking Up Resources (AWS CLI)

Puede utilizarla AWS CLI para enumerar los recursos que AWS Config ha descubierto.

Utilice el comando AWS Config service **`list-discovered-resources`**:

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
        }
```

Para ver los detalles de la configuración de un recurso que aparece en la respuesta, utilice el comando `get-resource-config-history` y especifique el tipo y el ID de recurso. Para ver un ejemplo de este comando y la respuesta de AWS Config, consulteVisualización del historial de configuración.

Looking up Resources (API)

Especifica un tipo de recurso y AWS Config devuelve una lista de identificadores de recursos para los recursos de ese tipo. Para obtener más información, consulta ResourceIdentifier en la AWS Config Referencia de la API de .

Utilice la acción ListDiscoveredResources.

Para obtener los detalles de la configuración de un recurso que aparece en la respuesta, utilice la acción GetResourceConfigHistory y especifique el tipo y el ID de recurso.

Visualización de la información de cumplimiento y los resultados de la evaluación de sus AWS recursos con AWS Config

> **Important**
>
> Para obtener informes precisos sobre el estado de cumplimiento, debe registrar el tipo de recurso de `AWS::Config::ResourceCompliance`. Para obtener más información, consulte AWS Recursos de grabación.

Puede utilizar la AWS Config consola o AWS SDKs ver la información de conformidad y los resultados de la evaluación de sus recursos.

Temas

- Visualización de la conformidad (consola)
- Visualización del cumplimiento (AWS SDKs)

Visualización de la conformidad (consola)

Visualización de la conformidad (consola)

1. Inicie sesión en la AWS Config consola Consola de administración de AWS y ábrala en https://console.aws.amazon.com/config/casa.
2. En el Consola de administración de AWS menú, compruebe que el selector de región esté configurado en una región que admita AWS Config reglas. Para ver una lista de las regiones

admitidas, consulte Regiones y puntos de enlace de AWS Config en la Referencia general de Amazon Web Services.

3. En el panel de navegación, elija Recursos. En la página Inventario de recursos, puede filtrar por categoría de recurso, tipo de recurso y estado de conformidad. Seleccione Incluir los recursos eliminados, si procede. En la tabla se muestra el identificador de recurso para el tipo de recurso y el estado de conformidad de ese recurso. El identificador de recursos puede ser un ID o un nombre de recurso.
4. Elija un recurso de la columna del identificador de recursos.
5. Elija el botón Escala de tiempo del recurso. Puede filtrar por eventos de configuración, eventos de conformidad o CloudTrail eventos.

> **Note**
>
> O bien, en la página Inventario de recursos, puede hacer clic directamente en el nombre del recurso. Para acceder a la escala de tiempo del recurso desde la página de detalles del recurso, elija el botón Escala de tiempo del recurso.

También puede ver la conformidad de sus recursos a través de búsquedas en la página Resource inventory. Para obtener más información, consulte Búsqueda de recursos descubiertos por AWS Config.

Visualización del cumplimiento (AWS SDKs)

Para obtener información sobre el cumplimiento de sus AWS recursos

Los siguientes ejemplos de código muestran cómo utilizar `DescribeComplianceByResource`.

CLI

AWS CLI

Para obtener información sobre el cumplimiento de sus AWS recursos

El siguiente comando devuelve la información de conformidad de cada instancia EC2 grabada por AWS Config y que infringe una o más reglas:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

En el resultado, el valor de cada atributo de `CappedCount` indica cuántas reglas infringe el recurso. Por ejemplo, el siguiente resultado indica que la instancia `i-1a2b3c4d` infringe dos reglas.

Salida:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeComplianceByResourcela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se revisa el tipo de recurso **`AWS::SSM::ManagedInstanceInventory`** para el tipo de cumplimiento COMPLIANT.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Salida:

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Para obtener más información sobre la API, consulte DescribeComplianceByResource Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se revisa el tipo de recurso **`AWS::SSM::ManagedInstanceInventory`** para el tipo de cumplimiento COMPLIANT.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Salida:

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Para obtener más información sobre la API, consulte DescribeComplianceByResourcela referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener el resumen de conformidad de sus recursos AWS

Los siguientes ejemplos de código muestran cómo utilizar `GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Resumen de conformidad para todos los tipos de recursos

El siguiente comando devuelve el número de AWS recursos que no cumplen y el número que lo son:

```
aws configservice get-compliance-summary-by-resource-type
```

En el resultado, el valor de cada atributo `CappedCount` indica el número de recursos conformes y el de no conformes.

Salida:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Obtención del resumen de conformidad de un tipo de recurso específico

El comando siguiente devuelve el número de instancias de EC2 no conformes y el número de las conformes:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

En el resultado, el valor de cada atributo `CappedCount` indica el número de recursos conformes y el de no conformes.

Salida:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByResourceTypela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se devuelve el número de recursos conformes y no conformes, y se convierte el resultado en json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
```

```
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByResourceType Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se devuelve el número de recursos conformes y no conformes, y se convierte el resultado en json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByResourceTypela referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener los resultados de la evaluación de un recurso AWS

Los siguientes ejemplos de código muestran cómo utilizar `GetComplianceDetailsByResource`.

CLI

AWS CLI

Para obtener los resultados de la evaluación de un AWS recurso

El siguiente comando devuelve los resultados de la evaluación para cada regla infringida por la instancia de EC2 `i-1a2b3c4d`:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Salida:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte GetComplianceDetailsByResourcela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Este ejemplo devuelve los resultados de la evaluación de un recurso determinado.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Salida:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Para obtener más información sobre la API, consulte GetComplianceDetailsByResource Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Este ejemplo devuelve los resultados de la evaluación de un recurso determinado.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Salida:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Para obtener más información sobre la API, consulte GetComplianceDetailsByResourcela referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Ver el historial de cumplimiento de sus AWS recursos con AWS Config

> **Important**
>
> El tipo de recurso `AWS::Config::ResourceCompliance` se utiliza para almacenar resultados históricos de cumplimiento de recursos. No es necesario registrar este tipo de recurso para que las reglas de Config evalúen los recursos o para ver el estado de cumplimiento actual en la consola.
>
> El registro de `AWS::Config::ResourceCompliance` solo le permite ver los cambios históricos de cumplimiento a lo largo del tiempo en la cronología de los recursos. Si no necesita datos de cumplimiento históricos, puede excluir este tipo de recurso. Para obtener más información sobre cómo seleccionar los recursos para grabar, consulte AWS Recursos de grabación.

Puede ver la configuración, las relaciones y el número de cambios realizados en un recurso en la AWS Config consola. Puede ver el historial de configuración de un recurso utilizando AWS CLI.

Temas

- Visualización del historial de conformidad (consola)
- Visualización del historial de conformidad (AWS CLI)
- Visualización del cronograma del historial de conformidad para recursos y reglas

Visualización del historial de conformidad (consola)

Visualización del historial de conformidad con la consola

Cuando busca recursos en la página Inventario de recursos, seleccione el nombre o ID del recurso en la columna del identificador de recurso para ver la página de detalles del recurso. La página de detalles proporciona información sobre la configuración, las relaciones y el número de cambios realizados en dicho recurso.

Para acceder a la escala de tiempo del recurso desde la página de detalles del recurso, elija el botón Escala de tiempo del recurso. La línea de temporal de recursos captura los cambios como `ConfigurationItems` a lo largo de un periodo de tiempo para un recurso específico. Puede filtrar por eventos de configuración, eventos de conformidad o CloudTrail eventos.

Visualización del historial de conformidad (AWS CLI)

Visualización del historial de conformidad mediante el AWS CLI

Los elementos de configuración que se AWS Config registran se entregan al canal de entrega especificado bajo demanda como una instantánea de la configuración y como un flujo de configuración. Puede utilizarla AWS CLI para ver el historial de los elementos de configuración de cada recurso.

Visualización del historial de configuración

Introduzca el comando `get-resource-config-history` y especifique el tipo de recurso y el ID de recurso; por ejemplo:

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
```

```
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

Para obtener una explicación detallada de los campos de respuesta, consulte Components of a Configuration Item y Tipos de recursos compatibles para AWS Config.

Ejemplo del historial de configuración de Amazon EBS de AWS Config

AWS Config genera un conjunto de archivos, cada uno de los cuales representa un tipo de recurso y enumera todos los cambios de configuración de los recursos de ese tipo que AWS Config se están grabando. AWS Config exporta este historial de configuración centrado en los recursos como un objeto en el bucket de Amazon S3 que especificó al habilitarlo. AWS Config El archivo del historial de configuración de cada tipo de recurso contiene los cambios que se han detectado para los recursos de ese tipo desde que se ha entregado el último archivo del historial. Por lo general, los archivos de historial se entregan cada seis horas.

A continuación, se muestra un ejemplo del contenido del objeto de Amazon S3 que describe el historial de configuración de todos los volúmenes de Amazon Elastic Block Store en la región actual para la Cuenta de AWS. Los volúmenes en esta cuenta incluyen `vol-ce676ccc` y `vol-cia007c`. El volumen `vol-ce676ccc` tenía dos cambios de configuración desde la entrega del archivo de historial anterior, mientras que el volumen `vol-cia007c` tenía un cambio.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
```

```
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-ad229edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04w292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
```

```
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-cia007c",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
```

```
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

Visualización del cronograma del historial de conformidad para recursos y reglas

AWS Config permite almacenar los cambios de estado de conformidad de los recursos evaluados por Reglas de AWS Config. El historial de conformidad de recursos se presenta en forma de una línea de tiempo. La línea de temporal captura los cambios como `ConfigurationItems` a lo largo de un periodo de tiempo para un recurso específico. Para obtener información sobre el contenido de`ConfigurationItem`, consulte ConfigurationItemla referencia de la AWS Config API.

Puede optar o no por registrar todos los tipos de recursos en AWS Config. Si ha optado por registrar todos los tipos de recursos, comienza a registrar AWS Config automáticamente el historial de conformidad de los recursos según lo evaluado por Reglas de AWS Config. De forma predeterminada, AWS Config registra los cambios de configuración de todos los recursos compatibles. También puede seleccionar solo el tipo de recurso del historial de conformidad específico del recurso: `AWS::Config::ResourceCompliance`. Para obtener más información, consulte Grabación de AWS registros.

Viewing Resource Timeline Using Resources

Acceda a la línea temporal de los recursos seleccionando un recurso específico en la página del inventario de recursos.

1. Seleccione los recursos en el panel de navegación izquierdo.
2. En la página Inventario de recursos, puede filtrar por categoría de recurso, tipo de recurso y estado de conformidad. Seleccione Incluir los recursos eliminados, si procede.

   En la tabla se muestra el identificador de recurso para el tipo de recurso y el estado de conformidad de ese recurso. El identificador de recursos puede ser un ID o un nombre de recurso.
3. Elija un recurso de la columna del identificador de recursos.
4. Elija el botón Escala de tiempo del recurso. Puede filtrar por eventos de configuración, eventos de conformidad o CloudTrail eventos.

> **Note**
>
> O bien, en la página Inventario de recursos, puede hacer clic directamente en el nombre del recurso. Para acceder a la escala de tiempo del recurso desde la página de detalles del recurso, elija el botón Escala de tiempo del recurso.

Viewing Resource Timeline Using Rules

Acceda a la línea temporal de conformidad seleccionando una regla específica desde la página Regla.

1. Seleccione las reglas en el panel de navegación izquierdo.
2. En la página Regla, haga clic en el nombre de la regla que valúa sus recursos pertinentes. Si no aparece ninguna regla en la pantalla, añada reglas utilizando el botón Add rule (Añadir regla).
3. En la página de detalles de la regla, seleccione los recursos de la tabla de recursos evaluados.
4. Seleccione el botón Cronograma de recursos. Aparece el cronograma de recursos.

Consulta el historial de conformidad de sus recursos AWS

Consulte el historial de conformidad de los recursos get-resource-config-history utilizando el tipo de recurso`AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

Debería ver una salida similar a esta:

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
```

```
      "relationshipName": "Is associated with "
     }
    ]
    "tags": {},
    "resourceType": "AWS::Config::ResourceCompliance",
    "resourceId": "AWS::S3::Bucket/configrules-bucket",
    "ConfigurationStateId": "1539799966921",
    "relatedEvents": [];
    "awsRegion": "us-west-2",
    "version": "1.3",
    "configurationItemMD5Hash": "",
    "supplementaryConfiguration": {},
    "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

    "configurationItemStatus": "ResourceDiscovered",
    "accountId": "AccountID"
   }
  ]
}
```

Etiquetado de los recursos de AWS Config

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Las etiquetas facilitan la administración, la búsqueda y el filtrado de recursos.

Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo, ya que puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado. Puede asignar una o varias etiquetas a sus recursos de AWS. Cada etiqueta dispone de un valor asociado.

Recomendamos que idee un conjunto de claves de etiqueta que cumpla sus necesidades para cada tipo de recurso. Mediante el uso de un conjunto coherente de claves de etiquetas, podrá administrar los recursos de AWS más fácilmente. Puede buscar y filtrar los recursos en función de las etiquetas que agregue.

Las etiquetas se interpretan estrictamente como una cadena de caracteres y no se asignan a los recursos automáticamente. Puede editar las claves y los valores de las etiquetas y también puede eliminar etiquetas de un recurso en cualquier momento. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Si añade una etiqueta con la misma clave que una etiqueta existente en ese recurso, el nuevo valor sobrescribirá al antiguo. Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

Puede trabajar con las etiquetas utilizando la AWS Command Line Interface (AWS CLI) y la API de AWS Config.

Restricciones relacionadas con el etiquetado

Se aplican las siguientes restricciones básicas a las etiquetas.

Restricción	Descripción
Número máximo de etiquetas por recurso	50
Longitud máxima de clave	128 caracteres Unicode en UTF-8
Longitud máxima de valor	256 caracteres Unicode en UTF-8
Restricción de prefijo	No utilice el prefijo `aws:` en los nombres o valores de las etiquetas, porque está reservado para uso de AWS. Los nombres y valores de etiquetas que tienen este prefijo no se pueden editar ni eliminar. Las etiquetas que tengan este prefijo no cuentan para el límite de etiquetas por recurso.
Restricciones de caracteres	Las etiquetas solo pueden contener letras Unicode, dígitos, espacios en blanco o estos símbolos: .: `_ . : / = + - @`

Administración de las etiquetas con las acciones de la API de AWS Config

Existen controles de acceso basados en etiquetas para estos tres recursos: `ConfigurationAggregator`, `AggregationAuthorization` y `ConfigRule`. Utilice lo siguiente para añadir, actualizar, listar y eliminar las etiquetas de los recursos.

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResource` y `UntagResource` requieren ciertos permisos de AWS Identity and Access Management (IAM) para controlar el acceso. Para obtener más información, consulte Controlling access based on tag keys en la Guía del usuario de IAM.

Evaluación de recursos con AWS Config reglas

Se utiliza AWS Config para evaluar los ajustes de configuración de AWS los recursos. Para ello, debe crear AWS Config reglas, que representan los valores de configuración ideales. AWS Config proporciona reglas personalizables y predefinidas denominadas reglas administradas para ayudarle a empezar.

Temas

- Consideraciones
- Compatibilidad de la región
- Componentes de una AWS Config regla
- AWS ConfigReglas de administradas
- AWS Config Reglas personalizadas
- Roles vinculados a servicios de AWS Config
- Administración de AWS Config reglas en todas las cuentas de su organización
- Añadir AWS Config reglas
- Actualización de AWS Config reglas
- Eliminar AWS Config reglas
- Visualización de los detalles y la información de cumplimiento de sus AWS Config reglas
- Activar la evaluación proactiva de AWS Config las reglas
- Envío de evaluaciones de reglas a Security Hub (CSPM)
- Evaluación de sus recursos con AWS Config reglas
- Eliminar los resultados de la evaluación de AWS Config las reglas
- Solución de problemas relacionados con las reglas AWS Config

Consideraciones

Cost Considerations

> Para obtener más información sobre los costos asociados al registro de recursos, consulte Precios de AWS Config.

Recomendación: considere excluir el tipo de recurso **`AWS::Config::ResourceCompliance`** del registro antes de eliminar reglas

Al eliminar las reglas, se crean elementos de configuración (CIs) `AWS::Config::ResourceCompliance` que pueden afectar a los costes del registrador de configuración. Si elimina reglas que evalúan un gran número de tipos de recursos, esto puede provocar un aumento en el número de CIs registros.

Para evitar los costos asociados, puede optar por deshabilitar el registro para el tipo de recurso `AWS::Config::ResourceCompliance` antes de eliminar reglas y volver a habilitarlo una vez eliminadas las reglas.

Sin embargo, dado que la eliminación de reglas es un proceso asincrónico, puede tardar una hora o más en completarse. Durante el tiempo en que el registro esté deshabilitado para `AWS::Config::ResourceCompliance`, las evaluaciones de reglas no se registrarán en el historial de recursos asociado.

AWS Config recomienda sopesar estos factores antes case-by-case de decidir cómo proceder a eliminar las reglas.

Recomendación: Añada lógica para gestionar la evaluación de los recursos eliminados para reglas de Lambda personalizadas

Al crear reglas lambda AWS Config personalizadas, se recomienda encarecidamente añadir lógica para gestionar la evaluación de los recursos eliminados.

Cuando los resultados de la evaluación se identifiquen como `NOT_APPLICABLE`, significa que se eliminarán y depurarán. Si NO están marcados como`NOT_APPLICABLE`, los resultados de la evaluación permanecerán sin cambios hasta que se elimine la regla, lo que puede provocar un aumento inesperado en la creación de CIs for `AWS::Config::ResourceCompliance` al eliminar la regla.

Para obtener información sobre cómo configurar reglas lambda AWS Config personalizadas `NOT_APPLICABLE` para que se devuelvan en el caso de los recursos eliminados, consulte Administrar los recursos eliminados con reglas lambda AWS Config personalizadas.

Recomendación: Proporcione los recursos disponibles para las reglas de Lambda personalizadas

AWS Config Las reglas Lambda personalizadas pueden provocar un número elevado de invocaciones a funciones Lambda si la regla no se limita a uno o más tipos de recursos. Para evitar el aumento de actividad asociado a su cuenta, es muy recomendable que proporcione

recursos disponibles para las reglas de Lambda personalizadas. Si no selecciona ningún tipo de recurso, la regla invocará la función de Lambda para todos los recursos de la cuenta.

Other considerations

Valores predeterminados para las reglas administradas

Los valores predeterminados especificados para las reglas administradas se rellenan automáticamente solo cuando se utiliza la consola. AWS No se proporcionan valores predeterminados para la API, la CLI o el SDK.

Retrasos en el registro de elementos de configuración

AWS Config por lo general, registra los cambios de configuración de los recursos inmediatamente después de detectar un cambio o con la frecuencia que especifique. Aunque el sistema hace todo lo posible porque sea así, a veces puede tardar más tiempo. Por ejemplo, un tipo de recurso con retrasos conocidos es `AWS::SecretsManager::Secret`. Este tipo de recurso es un ejemplo y esta lista no es exhaustiva.

Políticas y resultados de cumplimiento

Las políticas de IAM y otras políticas gestionadas AWS Organizations pueden afectar a la disponibilidad AWS Config de permisos para registrar los cambios de configuración de los recursos. Además, las reglas evalúan directamente la configuración de un recurso y no tienen en cuenta estas políticas al ejecutar las evaluaciones. Asegúrese de que las políticas en vigor se ajusten a la forma en que piensa utilizar AWS Config.

Compatibilidad con el etiquetado para tipos de recursos

Si un tipo de recurso no admite el etiquetado o no incluye información sobre las etiquetas en la respuesta de la API que describe, AWS Config no capturará los datos de las etiquetas de los elementos de configuración (CIs) de ese tipo de recurso. AWS Config seguirá registrando estos recursos. Sin embargo, cualquier funcionalidad que dependa de los datos de las etiquetas no funcionará. Esto afecta al filtrado, la agrupación o la evaluación del cumplimiento que se basan en los datos de las etiquetas.

Los buckets de directorio no están admitidos

Las reglas administradas solo admiten buckets de uso general al evaluar los recursos de Amazon Simple Storage Service (Amazon S3). Para obtener más información sobre los buckets de uso general y los buckets de directorio, consulte la información general sobre los buckets y los buckets de directorio en la Guía del usuario de Amazon S3.

Reglas administradas y tipos de recursos de IAM globales

Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.

Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.

A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Compatibilidad de la región

Actualmente, la función de AWS Config regla se admite en las siguientes AWS regiones. Para ver una lista de AWS Config las reglas individuales que se admiten en cada región, consulte la Lista de reglas AWS Config administradas por disponibilidad regional.

Nombre de la región	Región	Punto de conexión	Protocolo	
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS	
Este de EE. UU. (Norte de Virginia)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS	

Nombre de la región	Región	Punto de conexión	Protocolo
Oeste de EE. UU. (Norte de California)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Tailandia)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
México (centro)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

En las siguientes regiones se admite la implementación de AWS Config reglas en las cuentas de los miembros de una AWS organización.

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Este de EE. UU. (Norte de Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Norte de California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia-Pacífico	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
(Hyderabad)			
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
Asia-Pacífico (Tailandia)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
México (centro)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Componentes de una AWS Config regla

AWS Config las reglas evalúan los ajustes de configuración de sus AWS recursos. En esta página se describen los componentes de una regla.

Temas

- Cómo funcionan AWS Config las reglas
- Tipos de desencadenadores
- Modos de evaluación
- AWS Config Metadatos de reglas

Cómo funcionan AWS Config las reglas

Aunque AWS Config realiza un seguimiento continuo de los cambios de configuración que se producen en los recursos, comprueba si estos cambios infringen alguna de las condiciones de las reglas. Si un recurso no cumple con la regla, AWS Config marca el recurso y la regla como no conformes.

Hay cuatro posibles resultados de evaluación para una AWS Config regla.

Resultado de la evaluación	Descripción
`COMPLIANT`	La regla cumple las condiciones de la comprobación de cumplimiento.
`NON_COMPLIANT`	La regla no cumple las condiciones de la comprobación de cumplimiento.
`ERROR`	Uno de los required/optional parámetros no es válido, no es del tipo correcto o tiene un formato incorrecto.
`NOT_APPLICABLE`	Se utiliza para filtrar los recursos a los que no se puede aplicar la lógica de la regla. Por ejemplo, la alb-desync-mode-checkregla solo comprueba los balanceadores de carga de aplicaciones e ignora los balanceadores de carga de red y los balanceadores de carga de puerta de enlace.

Por ejemplo, cuando se crea un EC2 volumen, AWS Config puede evaluarlo según una regla que exige el cifrado de los volúmenes. Si el volumen no está cifrado, AWS Config marca el volumen y la regla como no conformes. AWS Config también puede comprobar todos sus recursos para conocer los requisitos de toda la cuenta. Por ejemplo, AWS Config puede comprobar si el número de EC2 volúmenes de una cuenta se mantiene dentro del total deseado o si una cuenta los utiliza AWS CloudTrail para el registro.

Tipos de desencadenadores

Tras añadir una regla a su cuenta, AWS Config compara sus recursos con las condiciones de la regla. Tras esta evaluación inicial, AWS Config continúa realizando evaluaciones cada vez que se activa una. Los desencadenadores de evaluaciones están definidos como parte de la regla, y pueden incluir los siguientes tipos.

Tipo de desencadenador	Descripción
Cambios de configuración	AWS Config ejecuta las evaluaciones de la regla cuando hay un recurso que coincide con el alcance de la regla y se produce un cambio en la configuración del recurso. La evaluación se ejecuta después de AWS Config enviar una notificación de cambio de elemento de configuración. Usted elige qué recursos activan la evaluación al definir el ámbito de la regla. El ámbito puede incluir lo siguiente: • Uno o varios tipos de recursos • Una combinación de un tipo de recurso y un ID de recurso • Una combinación de una clave de etiqueta y un valor • Cuando se crea, se actualiza o se elimina cualquier recurso registrado AWS Config ejecuta la evaluación cuando detecta un cambio en un recurso que coincide con el alcance de la regla. Puede utilizar el ámbito para definir los recursos que activan evaluaciones.
Periódico	AWS Config ejecuta las evaluaciones de la regla con la frecuencia que usted elija; por ejemplo, cada 24 horas.
Híbrido	Algunas reglas tienen cambios de configuración y desencadenadores periódicos. Para estas reglas, AWS Config evalúa sus recursos

Tipo de desencadenador	Descripción
	cuando detecta un cambio de configuración y también con la frecuencia que especifique.

Modos de evaluación

Hay dos modos de evaluación de las AWS Config reglas.

Modo de evaluación	Descripción
Proactiva	Utilice una evaluación proactiva para evaluar los recursos antes de que se implementen. Esto le permite evaluar si un conjunto de propiedades de un recurso, si se utiliza para definir un AWS recurso, cumple o no lo cumple, dado el conjunto de reglas proactivas que tiene en su cuenta en su región.
Detective	Utilice la evaluación de detectives para evaluar los recursos que ya se han implementado. Esto le permite evaluar los ajustes de configuración de los recursos existentes.

> **Note**
>
> Las reglas proactivas no corrigen los recursos que están marcados como NON_COMPLIANT ni impiden su implementación.

Para obtener más información, consulte Activar la evaluación proactiva de las AWS Config reglas.

Lista de reglas administradas con una evaluación proactiva

Para obtener una lista de las reglas administradas que admiten la evaluación proactiva, consulte la lista de reglas AWS Config administradas por modo de evaluación.

Lista de tipos de recursos compatibles para la evaluación proactiva

La siguiente es una lista de los tipos de recursos que se admiten para la evaluación proactiva:

- `AWS::EC2::EIP`

AWS Config Metadatos de reglas

AWS Config las reglas pueden contener los siguientes metadatos mutables:

defaultName

El defaultName es el nombre que recibirán las instancias de una regla de forma predeterminada.

description

La description de la regla proporciona el contexto de lo que evalúa la regla. La consola de AWS Config tiene un límite de 256 caracteres. Como práctica recomendada, la descripción de la regla debería empezar por “Comprueba si” e incluir una descripción del supuesto NON_COMPLIANT. Los nombres de los servicios deben escribirse completos empezando AWS por Amazon cuando se mencionen por primera vez en la descripción de la regla. Por ejemplo, AWS CloudTrail o Amazon CloudWatch en lugar de CloudTrail o CloudWatch para el primer uso. Los nombres de los servicios se pueden abreviar después.

scope

El scope determina los tipos de recursos a los que se dirige la regla. Para obtener una lista de tipos de recursos compatibles, consulte Tipos de recursos compatibles.

compulsoryInputParameterDetalles

Los compulsoryInputParameter detalles se utilizan para los parámetros necesarios para que una regla pueda evaluarse. Por ejemplo, la regla de `access-keys-rotated` administrada incluye `maxAccessKeyAge` como parámetro obligatorio. Si un parámetro es obligatorio, no se marcará como (opcional). Para cada parámetro, se debe especificar un tipo Los tipos pueden ser «String», «int», «double», «CSV», «boolean» y "StringMap».

optionalInputParameterDetalles

Los optionalInputParameter detalles se utilizan para los parámetros que son opcionales para que una regla realice su evaluación. Por ejemplo, la regla de `elasticsearch-logs-to-cloudwatch` administrada incluye `logTypes` como parámetro opcional. Para cada parámetro,

se debe especificar un tipo El tipo puede ser «String», «int», «double», «CSV», «boolean» y "StringMap».

supportedEvaluationModes

supportedEvaluationModes Determina cuándo se evaluarán los recursos, ya sea antes de que se haya implementado un recurso o después de que se haya implementado.

`DETECTIVE` se utiliza para evaluar los recursos que ya se han implementado. Esto le permite evaluar los valores de configuración de los recursos existentes. `PROACTIVE` se utiliza para evaluar los recursos antes de que se hayan implementado.

Esto le permite evaluar si un conjunto de propiedades de un recurso, si se utiliza para definir un AWS recurso, cumple o no lo es, dado el conjunto de reglas proactivas que tiene en su cuenta en su región.

Puede especificar el tipo « supportedEvaluationModes para» `DETECTIVEPROACTIVE`, o ambos `DETECTIVE` «y». `PROACTIVE` Debe especificar un modo de evaluación; este campo no puede permanecer vacío.

> **Note**
>
> Las reglas proactivas no corrigen los recursos que están marcados como NON_COMPLIANT ni impiden su implementación.

AWS ConfigReglas de administradas

AWS Config proporciona reglas administradas de AWS, que son reglas personalizables y predefinidas que AWS Config utiliza para evaluar si los recursos de AWS se ajustan a las prácticas recomendadas. Por ejemplo, podría utilizar una regla administrada para empezar a evaluar de forma rápida si sus volúmenes de Amazon Elastic Block Store (Amazon EBS) están cifrados o si se aplican etiquetas específicas a los recursos.

La consola de AWS Config le guiará por el proceso de configuración y activación de una regla administrada. También puede utilizar AWS Command Line Interface o la API de AWS Config para pasar el código JSON que define la configuración de una regla administrada.

Puede personalizar el comportamiento de una regla administrada para adaptarla a sus necesidades. Por ejemplo, puede definir el ámbito de la regla para restringir qué recursos inician una evaluación para la regla como, por ejemplo, volúmenes o instancias EC2.

Puede personalizar los parámetros de la regla para definir los atributos que deben tener los recursos para cumplir la regla. Por ejemplo, puede personalizar un parámetro para especificar que el grupo de seguridad debería bloquear el tráfico entrante a un número de puerto específico.

Antes de utilizar reglas administradas, consulte Consideraciones.

Temas

- Lista de reglas AWS Config administradas
- Lista de reglas AWS Config administradas por modo de evaluación
- Lista de reglas AWS Config administradas por tipo de activador
- Lista de reglas AWS Config administradas por región y disponibilidad
- Creación de reglas AWS Config administradas con AWS CloudFormation plantillas

Lista de reglas AWS Config administradas

AWS Config actualmente admite las siguientes reglas administradas. Antes de usar estas reglas, consulte Consideraciones.

Temas

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para encabezado
- alb-http-to-https-comprobación de redireccionamiento
- alb-internal-scheme-check

- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitada para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-predeterminado-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc

- apprunner-service-ip-address-verificación de tipo
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-en reposo
- appsync-cache-ct-encryption-en tránsito
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault

- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2.
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip deshabilitada
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum- control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check

- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configurado
- cloudfront-distribution-key-group-habilitado
- cloudfront-no-deprecated-ssl-protocolos
- cloudfront-origin-access-identity-habilitado
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-habilitado para oac
- frente a nubos-s3- origin-access-control-enabled
- frente a nubos-s3- origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encriptado
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes -S3- bucket-access-logging
- rastro de nubes -S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-registros habilitados
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitada para validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado de 3 registros
- codebuild-project-source-repo-comprobación de URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-actualización de instancias
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-turno desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-con seguridad habilitada
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado

- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro

- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec-2 capacity-reservation-tagged
- ec-2 carrier-gateway-tagged
- ec2- activado client-vpn-connection-log
- ec-2 client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize

- ec-2 dhcp-options-tagged
- ec-2 ebs-encryption-by-default
- ec2- activado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec-2 instance-detailed-monitoring-enabled
- ec-2 -ami instance-launched-with-allowed
- ec2- -administrador instance-managed-by-systems
- ec-2 instance-multiple-eni-check
- ec-2 instance-no-public-ip
- ec-2 instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -deshabilitado launch-template-public-ip
- ec-2 launch-template-tagged
- ec-2 managedinstance-applications-blacklisted
- ec-2 managedinstance-applications-required
- ec2- -comprobar managedinstance-association-compliance-status
- ec-2 managedinstance-inventory-blacklisted
- ec2- -comprobar managedinstance-patch-compliance-status
- ec-2 managedinstance-platform-check
- ec-2 meets-restore-time-target
- ec2- network-insights-access-scope -análisis-etiquetado
- ec2- -etiquetado network-insights-access-scope
- ec-2 network-insights-analysis-tagged
- ec-2 network-insights-path-tagged
- ec-2 no-amazon-key-pair
- ec-2 paravirtual-instance-check

- ec-2 prefix-list-tagged
- ec2- -bóveda con huecos resources-in-logically-air
- plan ec2 resources-protected-by-backup
- ec-2 security-group-attached-to -es
- ec2- -eni-periódico security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec-2 token-hop-limit-check
- ec-2 traffic-mirror-filter-description
- ec-2 traffic-mirror-filter-tagged
- ec-2 traffic-mirror-session-description
- ec-2 traffic-mirror-session-tagged
- ec-2 traffic-mirror-target-description
- ec-2 traffic-mirror-target-tagged
- ec2- -attach-desactivado transit-gateway-auto-vpc
- ec2- -etiquetado transit-gateway-multicast-domain
- ec-2 volume-inuse-check
- ec-2 vpn-connection-logging-enabled
- ec-2 vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-cifrado activado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-comprobación de modo
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio-raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión

- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitada para autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to- vigilancia en la nube
- elastic-beanstalk-managed-updates-habilitado
- elb 2- acm-certificate-required
- elb 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required

- elb-cross-zone-load-habilitado para el equilibrio
- elb-custom-security-policy-comprobación de SSL
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-comprobación de SSL
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-IP
- emr-security-configuration-encryption-descanso
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-cifrado activado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración-existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged

- frauddetector-variable-tagged
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- servicio de guardia -ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones

- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-saml-provider-tagged
- iam-server-certificate-expiration-comprobar
- iam-server-certificate-tagged
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-no-policies-comprobar
- iam-user-unused-credentials-comprobar
- restricted-ssh
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- ec-2 instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged

- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación

- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public- anula - desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-comprobación-descubrimiento
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitado para la actualización
- mq-auto-minor-version-habilitado para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado

- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requerido-tls
- msk-unrestricted-access-check
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a Cloudwatch
- rds-automatic-minor-version-habilitado para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descanso
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar

- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-a Cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multifunción
- redshift-default-admin-check
- redshift-default-db-name-comprobar

- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-verificación de nombres
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs-a Cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- health-check-tagged
- ruta 53- hosted-zone-tagged
- ruta 53- query-logging-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociación-etiquetada resolver-firewall-rule-group
- ruta 53- - etiquetada resolver-firewall-rule-group
- ruta 53- resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-registros habilitados
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle -reglas-check
- solo access-point-in-vpc s3
- bloques s3 access-point-public-access -
- bloques s3 account-level-public-access -
- s3- account-level-public-access -bloques-periódicos
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited

- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- plano resources-protected-by-backup s3
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged

- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-PVC
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-habilitado para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitada
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-default-security-group-cerrado
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- guerra 2- rulegroup-logging-enabled

- guerra 2- rulegroup-not-empty
- guerra 2- webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-vacío
- waf-global-rule-not-vacío
- waf-global-webacl-not-vacío
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

access-keys-rotated

Comprueba si las claves de acceso de IAM activas rotan (se modifican) en el número de días especificados en `maxAccessKeyAge`. La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.

> **Warning**
>
> No proporcione sus claves de acceso a terceros no autorizados, ni siquiera para que le ayuden a buscar sus identificadores de cuenta. De este modo, podrías dar a alguien acceso permanente a tu cuenta. La práctica recomendada de seguridad es eliminar las contraseñas y claves de acceso cuando los usuarios ya no las necesiten.

> **Note**
>
> Tipo de recurso marcado como no conforme en la consola
> Si esta regla determina que alguna de tus claves de acceso no es compatible, el tipo de `AWS::IAM::User` recurso también se marcará como no compatible en la AWS consola.
> Reglas administradas y tipos de recursos de IAM globales

Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.

Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.

A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Limitaciones

Esta regla no se aplica a las claves de acceso de los usuarios raíz de la AWS cuenta. Para eliminar o cambiar las claves de acceso del usuario raíz, utilice sus credenciales de usuario raíz para iniciar sesión en la página Mis credenciales de seguridad, Consola de administración de AWS en la dirección arrobahttps://aws.amazon.com/console/.

Identificador: ACCESS_KEYS_ROTATED

Tipos de recursos: AWS::IAM::User

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

maxAccessKeyEdad, Tipo: int, Valor predeterminado: 90

Número máximo de días sin rotación. El valor predeterminado es 90.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

account-part-of-organizations

Comprueba si una AWS cuenta forma parte de AWS Organizations. La regla no es compatible si una AWS cuenta no forma parte de Organizations o si el ID de la cuenta maestra de AWS AWS Organizations no coincide con el parámetro de la regla. `MasterAccountId`

> **Note**
>
> Reglas administradas y tipos de recursos de IAM globales
> Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.
> Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.
> A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Identificador: ACCOUNT_PART_OF_ORGANIZATIONS

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles excepto la región de China (Pekín)

Parámetros:

MasterAccountId (Opcional), Tipo: cadena

El ID de la cuenta maestra de una AWS cuenta.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

acmpca-certificate-authority-tagged

Comprueba si las autoridades de certificación de CA AWS privadas tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: ACMPCA_CERTIFICATE_AUTHORITY_TAGGED

Tipos de recursos: AWS::ACMPCA::CertificateAuthority

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

acm-certificate-expiration-check

Comprueba si los certificados de AWS Certificate Manager de su cuenta están marcados como vencidos en el número de días especificado. Los certificados que proporciona ACM se renuevan automáticamente. ACM no renueva automáticamente los certificados que se importan. La regla es NON_COMPLIANT si sus certificados están a punto de caducar.

Identificador: ACM_CERTIFICATE_EXPIRATION_CHECK

Tipos de recursos: AWS::ACM::Certificate

Tipo de desencadenador: cambios de configuración y periódicos

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

daysToExpiration (Opcional), Tipo: int, Valor predeterminado: 14

> Especifica el número de días antes de que la regla marque el certificado de ACM como no conforme.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

acm-certificate-rsa-check

Comprueba si los certificados RSA administrados por AWS Certificate Manager (ACM) tienen una longitud de clave de al menos «2048» bits. La regla no es compatible si la longitud mínima de la clave es inferior a 2048 bits.

Identificador: ACM_CERTIFICATE_RSA_CHECK

Tipos de recursos: AWS::ACM::Certificate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

acm-pca-root-ca-deshabilitado

Comprueba si la autoridad de certificación AWS AWS privada (CA privada) tiene una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

Identificador: ACM_PCA_ROOT_CA_DISABLED

Tipos de recursos: AWS::ACMPCA::CertificateAuthority

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

exento (opcional) CAArns , Tipo: CSV

> Lista separada por comas de nombres de recursos de Amazon (ARN) de las CA que se pueden habilitar. Este valor se puede proporcionar para otras CAs, como las CA raíz CAs o intermedias específicas que se pueden habilitar.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

active-mq-supported-version

Comprueba si un agente de ActiveMQ de Amazon MQ se ejecuta en una versión de motor mínima compatible que se haya especificado. La regla es NON_COMPLIANT si el agente de ActiveMQ no se ejecuta en la versión de motor mínima compatible que usted especifique.

Identificador: ACTIVE_MQ_SUPPORTED_VERSION

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

supportedEngineVersion, Tipo: cadena

> Valor de cadena de la regla para comprobar la versión de motor mínima compatible para el agente de ActiveMQ. Los agentes de ActiveMQ utilizan la especificación semántica de control de versiones X.Y.Z. X indica la versión principal, Y representa la versión secundaria y Z representa la versión del parche.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

alb-desync-mode-check

Comprueba si el equilibrador de carga de aplicación (ALB) está configurado con un modo de mitigación de desincronización definido por el usuario. La regla es NON_COMPLIANT si el modo de mitigación de desincronización de ALB no coincide con el modo de mitigación de desincronización definido por el usuario.

Identificador: ALB_DESYNC_MODE_CHECK

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

desyncMode, Tipo: CSV

> Lista separada por comas, en la que los clientes pueden elegir un máximo de 2 valores entre: defensivo, más estricto y supervisión.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

alb-http-drop-invalid-habilitado para encabezado

Comprueba si la regla evalúa los balanceadores de carga de AWS aplicaciones (ALB) para garantizar que estén configurados para eliminar los encabezados http. La regla es NON_COMPLIANT si el valor de routing.http.drop_invalid_header_fields.enabled se establece en false.

Identificador: ALB_HTTP_DROP_INVALID_HEADER_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

alb-http-to-https-comprobación de redireccionamiento

Comprueba si el redireccionamiento de HTTP a HTTPS está configurado en todos los oyentes HTTP de los equilibradores de carga de aplicación. La regla es NON_COMPLIANT si uno o varios oyentes HTTP del equilibrador de carga de aplicación no tienen configurado el redireccionamiento de HTTP a HTTPS. La regla también es NON_COMPLIANT si uno o más oyentes HTTP realizan el reenvío a un oyente HTTP en lugar de la redirección.

Identificador: ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

alb-internal-scheme-check

Comprueba si un esquema del Equilibrador de carga de aplicación es interno. La regla es NON_COMPLIANT si el esquema de configuración no se establece como interno.

Identificador: ALB_INTERNAL_SCHEME_CHECK

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

alb-listener-tagged

Comprueba si los oyentes del Equilibrador de carga de aplicación tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: ALB_LISTENER_TAGGED

Tipos de recursos: AWS::ElasticLoadBalancingV2::Listener

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

alb-tagged

Comprueba si los Equilibradores de carga de aplicación tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: ALB_TAGGED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

alb-waf-enabled

Comprueba si el firewall de aplicaciones web (WAF) está activado en los balanceadores de carga de aplicaciones (). ALBs Esta regla no cumple con los requisitos si la clave: waf.enabled está establecida en false.

Identificador: ALB_WAF_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

wafWebAclID (opcional), Tipo: CSV

> Lista separada por comas de ID de ACL web (para WAF) o ARN de ACL web (para WAFV2) que comprueba la asociación de ALB

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

amplify-app-branch-auto-habilitado para eliminar

Comprueba si las aplicaciones de AWS Amplify desconectan automáticamente una rama de Amplify Hosting cuando eliminas una rama de tu repositorio de Git. La regla NO ES COMPATIBLE si está configurada. EnableBranchAutoDeletion es falsa.

Identificador: AMPLIFY_APP_BRANCH_AUTO_DELETION_ENABLED

Tipos de recursos: AWS::Amplify::App

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

amplify-app-description

Comprueba si las aplicaciones de AWS Amplify tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: AMPLIFY_APP_DESCRIPTION

Tipos de recursos: AWS::Amplify::App

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

amplify-app-no-environment-variables

Comprueba que las aplicaciones de AWS Amplify no contengan variables de entorno. La regla NO ES COMPATIBLE si está configurada. EnvironmentVariables no es una lista vacía.

Identificador: AMPLIFY_APP_NO_ENVIRONMENT_VARIABLES

Tipos de recursos: AWS::Amplify::App

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

amplify-app-tagged

Comprueba si las aplicaciones de AWS Amplify tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: AMPLIFY_APP_TAGGED

Tipos de recursos: AWS::Amplify::App

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este)

AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

amplify-branch-description

Comprueba si las sucursales de AWS Amplify tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: AMPLIFY_BRANCH_DESCRIPTION

Tipos de recursos: AWS::Amplify::Branch

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

amplify-branch-performance-mode-habilitado

Comprueba si las sucursales de AWS Amplify tienen activado el modo de rendimiento. La regla NO ES COMPATIBLE si está configurada. EnablePerformanceMode es falsa.

Identificador: AMPLIFY_BRANCH_PERFORMANCE_MODE_ENABLED

Tipos de recursos: AWS::Amplify::Branch

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

amplify-branch-tagged

Comprueba si las sucursales de AWS Amplify tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: AMPLIFY_BRANCH_TAGGED

Tipos de recursos: AWS::Amplify::Branch

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

apigatewayv2-stage-description

Comprueba si todas las etapas de Amazon API Gateway V2 tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: APIGATEWAYV2 _STAGE_DESCRIPTION

Tipos de recursos: AWS::ApiGatewayV2::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

apigateway-stage-access-logs-habilitado

Comprueba si todas las etapas de Amazon API Gateway tienen habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.

Identificador: APIGATEWAY_STAGE_ACCESS_LOGS_ENABLED

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

apigateway-stage-description

Comprueba si todas las etapas de Amazon API Gateway tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: APIGATEWAY_STAGE_DESCRIPTION

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

api-gwv2- access-logs-enabled

Comprueba que todas las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.

Identificador: 2_ACCESS_LOGS_ENABLED API_GWV

Tipos de recursos: AWS::ApiGatewayV2::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Zúrich)) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

api-gwv2- authorization-type-configured

Comprueba si las rutas de la API de Amazon API Gateway V2 tienen un tipo de autorización establecido. Esta regla es NON_COMPLIANT si el tipo de autorización es NONE.

Identificador: 2_AUTHORIZATION_TYPE_CONFIGURED API_GWV

Tipos de recursos: AWS::ApiGatewayV2::Route

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Zúrich) Región

Parámetros:

authorizationType (opcional), Tipo: cadena

> Parámetro con el que comparar los tipos de autorización de las rutas de la API. Los parámetros de cadena que coincidan con CUSTOM, AWS_IAM y JWT son válidos.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

api-gwv2- -habilitada para métricas stage-default-route-detailed

Comprueba si todos los ajustes de ruta predeterminados de las etapas de Amazon API Gateway V2 tienen habilitadas las métricas detalladas. La regla no cumple con las normas si está configurada. defaultRouteSettings. detailedMetricsEnabled es falso.

Identificador: API_GWV 2_STAGE_DEFAULT_ROUTE_DETAILED_METRICS_ENABLED

Tipos de recursos: AWS::ApiGatewayV2::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

api-gw-associated-with-guerra

Comprueba si una etapa de la API de Amazon API Gateway utiliza una lista de control de acceso web (ACL web) de AWS WAF. La regla no cumple con los requisitos si no se utiliza una ACL web de AWS WAF o si una ACL AWS web utilizada no coincide con lo que aparece en el parámetro de la regla.

Identificador: _ASSOCIATED_WITH_WAF API_GW

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

WebAclArns (Opcional), Tipo: CSV

Lista separada por comas de nombres de recursos de Amazon ACL web () ARNs

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

api-gw-cache-enabled-y encriptado

Comprueba si todos los métodos de las etapas de Amazon API Gateway tienen la caché activada y cifrada. La regla es NON_COMPLIANT si algún método de una etapa de Amazon API Gateway no está configurada para el almacenamiento en caché o si la caché no está cifrada.

Identificador: _CACHE_ENABLED_AND_ENCRYPTED API_GW

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

api-gw-endpoint-type-comprobar

Comprueba si Amazon API Gateway APIs es del tipo especificado en el parámetro de regla`endpointConfigurationType`. La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.

Identificador: API_GW _ENDPOINT_TYPE_CHECK

Tipos de recursos: AWS::ApiGateway::RestApi

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

endpointConfigurationTypes, Tipo: CSV

Lista de permitidos separada por comas. endpointConfigurationTypes Los valores permitidos son REGIONAL, PRIVATE y EDGE.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

api-gw-execution-logging-habilitado

Comprueba que todos los métodos de las etapas de Amazon API Gateway tengan habilitado el registro. La regla es NON_COMPLIANT si el registro no está activado o si `loggingLevel` no es ERROR ni INFO.

Identificador: _EXECUTION_LOGGING_ENABLED API_GW

Tipos de recursos:, AWS::ApiGateway::Stage AWS::ApiGatewayV2::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de Asia Pacífico (Taipéi)

Parámetros:

loggingLevel (opcional), Tipo: cadena, Valor predeterminado: ERROR,INFO

Lista separada por comas de niveles de registro específicos (por ejemplo, ERROR, INFO o ERROR,INFO).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

api-gw-rest-api-etiquetado

Comprueba si los recursos de la API AWS ApiGateway REST tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de

etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: API_GW _REST_ API_TAGGED

Tipos de recursos: AWS::ApiGateway::RestApi

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

api-gw-ssl-enabled

Comprueba si una etapa de la API de REST utiliza un certificado SSL. La regla es NON_COMPLIANT si la etapa de la API de REST no tiene un certificado SSL asociado.

> **Note**
>
> Esta regla se devuelve `NOT_APPLICABLE` si la GetIntegrationAPI devuelve un tipo de integración que no sea el tipo `HTTP` as. Esta regla evalúa la configuración del certificado SSL en la configuración de la etapa de API Gateway, no en el estado de implementación real.

Identificador: _SSL_ENABLED API_GW

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de Asia Pacífico (Taipéi)

Parámetros:

Certificado IDs (opcional), Tipo: CSV

Lista separada por comas de certificados de cliente IDs configurados en una etapa de la API REST.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

api-gw-stage-tagged

Comprueba si los recursos de la AWS ApiGateway etapa tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: API_GW _STAGE_TAGGED

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

api-gw-xray-enabled

Comprueba si el rastreo de AWS X-Ray está habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

Identificador: _XRAY_ENABLED API_GW

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con reglas. AWS Config Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
```

```
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appconfig-application-description

Comprueba si AWS AppConfig las aplicaciones tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: APPCONFIG_APPLICATION_DESCRIPTION

Tipos de recursos: AWS::AppConfig::Application

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appconfig-application-tagged

Comprueba si AWS AppConfig las aplicaciones tienen etiquetas. También puede especificar claves de etiqueta para comprobar la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPCONFIG_APPLICATION_TAGGED

Tipos de recursos: AWS::AppConfig::Application

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appconfig-configuration-profile-tagged

Comprueba si los perfiles de AWS AppConfig configuración tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPCONFIG_CONFIGURATION_PROFILE_TAGGED

Tipos de recursos: AWS::AppConfig::ConfigurationProfile

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appconfig-configuration-profile-validators-no está vacío

Comprueba si un perfil de AWS AppConfig configuración incluye al menos un validador para la comprobación sintáctica o semántica a fin de garantizar que el despliegue de la configuración funcione según lo previsto. La regla es NON_COMPLIANT si la propiedad Validators es una matriz vacía.

Identificador: APPCONFIG_CONFIGURATION_PROFILE_VALIDATORS_NOT_EMPTY

Tipos de recursos: AWS::AppConfig::ConfigurationProfile

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appconfig-deployment-strategy-description

Comprueba si las estrategias de AWS AppConfig despliegue tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: APPCONFIG_DEPLOYMENT_STRATEGY_DESCRIPTION

Tipos de recursos: AWS::AppConfig::DeploymentStrategy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appconfig-deployment-strategy-minimum-final-bake-time

Comprueba si una estrategia AWS AppConfig de despliegue requiere el tiempo de cocción mínimo especificado. La regla es NON_COMPLIANT si la estrategia de implementación tiene un tiempo de incorporación final menor que el valor especificado en el parámetro de regla. El valor predeterminado es 30 minutos.

Identificador: APPCONFIG_DEPLOYMENT_STRATEGY_MINIMUM_FINAL_BAKE_TIME

Tipos de recursos: AWS::AppConfig::DeploymentStrategy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

minBakeTime (Opcional), Tipo: int, Valor predeterminado: 30

> El tiempo mínimo de cocción en minutos de la estrategia de AWS AppConfig despliegue para que se compruebe la regla. La regla es NON_COMPLIANT si el tiempo de incorporación es menor que el valor especificado en este parámetro. Los valores válidos van de 0 a 1440. El valor predeterminado es 30.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appconfig-deployment-strategy-replicate-a-ssm

Comprueba si las estrategias de AWS AppConfig despliegue guardan la estrategia de despliegue en un documento de AWS Systems Manager (SSM). La regla no cumple con las normas si está configurada. ReplicateTo no es 'SSM_DOCUMENT'.

Identificador: APPCONFIG_DEPLOYMENT_STRATEGY_REPLICATE_TO_SSM

Tipos de recursos: AWS::AppConfig::DeploymentStrategy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appconfig-deployment-strategy-tagged

Comprueba si las estrategias de AWS AppConfig despliegue tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPCONFIG_DEPLOYMENT_STRATEGY_TAGGED

Tipos de recursos: AWS::AppConfig::DeploymentStrategy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

includePredefinedSystemRecursos, Tipo: booleano, Valor predeterminado: False

Un valor booleano que especifica si se incluyen estrategias de implementación predefinidas para que la regla las compruebe. El valor predeterminado es false.

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appconfig-environment-description

Comprueba si AWS AppConfig los entornos tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: APPCONFIG_ENVIRONMENT_DESCRIPTION

Tipos de recursos: AWS::AppConfig::Environment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appconfig-environment-tagged

Comprueba si AWS AppConfig los entornos tienen etiquetas. También puede especificar claves de etiqueta para comprobar la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPCONFIG_ENVIRONMENT_TAGGED

Tipos de recursos: AWS::AppConfig::Environment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico

(Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appconfig-extension-association-tagged

Comprueba si las asociaciones de AWS AppConfig extensiones tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPCONFIG_EXTENSION_ASSOCIATION_TAGGED

Tipos de recursos: AWS::AppConfig::ExtensionAssociation

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appconfig-freeform-profile-config-almacenamiento

Comprueba si los perfiles de configuración de formato libre AWS AppConfig almacenan sus datos de configuración en AWS Secrets Manager o en un almacén de configuración AWS AppConfig alojado. La regla NO ES COMPATIBLE si está configurada. LocationUri no es un administrador de secretos ni está alojado.

Identificador: APPCONFIG_FREEFORM_PROFILE_CONFIG_STORAGE

Tipos de recursos: AWS::AppConfig::ConfigurationProfile

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appconfig-hosted-configuration-version-descripción

Comprueba si las versiones de la configuración AWS AppConfig alojada tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: APPCONFIG_HOSTED_CONFIGURATION_VERSION_DESCRIPTION

Tipos de recursos: AWS::AppConfig::HostedConfigurationVersion

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appflow-flow-tagged

Comprueba si los AppFlow flujos de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPFLOW_FLOW_TAGGED

Tipos de recursos: AWS::AppFlow::Flow

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), África (Ciudad del Cabo), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appflow-flow-trigger-type-comprobar

Comprueba si un AppFlow flujo de Amazon se ejecuta con el tipo de disparador especificado. La regla es NON_COMPLAINT si el flujo no se ejecuta con el tipo de desencadenador especificado en el parámetro de regla obligatorio.

Identificador: APPFLOW_FLOW_TRIGGER_TYPE_CHECK

Tipos de recursos: AWS::AppFlow::Flow

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), África (Ciudad del Cabo), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

triggerType, Tipo: CSV

Lista separada por comas de tipos de desencadenadores que la regla debe comprobar. Los valores válidos incluyen: «Programado», «Evento» y «OnDemand».

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appintegrations-event-integration-description

Comprueba si las integraciones de AppIntegrations eventos de Amazon tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe.

Identificador: APPINTEGRATIONS_EVENT_INTEGRATION_DESCRIPTION

Tipos de recursos: AWS::AppIntegrations::EventIntegration

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en África (Ciudad del Cabo), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appintegrations-event-integration-tagged

Comprueba si las integraciones de AppIntegrations eventos de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPINTEGRATIONS_EVENT_INTEGRATION_TAGGED

Tipos de recursos: AWS::AppIntegrations::EventIntegration

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en África (Ciudad del Cabo), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appmesh-gateway-route-tagged

Comprueba si las rutas de las puertas de enlace de AWS App Mesh tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPMESH_GATEWAY_ROUTE_TAGGED

Tipos de recursos: AWS::AppMesh::GatewayRoute

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appmesh-mesh-deny-tcp-reenvío

Comprueba si los proxies de las mallas del servicio AWS App Mesh no reenvían el tráfico TCP directamente a los servicios que no se implementan con un proxy definido en la malla. La regla no cumple con los requisitos de Configuration.spec. EgressFilter.Type está establecido en «ALLOW_ALL».

Identificador: APPMESH_MESH_DENY_TCP_FORWARDING

Tipos de recursos: AWS::AppMesh::Mesh

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appmesh-mesh-tagged

Comprueba si las mallas AWS App Mesh tienen etiquetas. También puede especificar claves de etiqueta para comprobar la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves

de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPMESH_MESH_TAGGED

Tipos de recursos: AWS::AppMesh::Mesh

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appmesh-route-tagged

Comprueba si las rutas de AWS App Mesh tienen etiquetas. También puede especificar claves de etiqueta para comprobar la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPMESH_ROUTE_TAGGED

Tipos de recursos: AWS::AppMesh::Route

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appmesh-virtual-gateway-backend-predeterminado-tls

Comprueba si los valores predeterminados del backend de las puertas de enlace virtuales de AWS App Mesh requieren que las puertas de enlace virtuales se comuniquen con todos los puertos mediante TLS. La regla no cumple con los requisitos de Configuration.spec. BackendDefaults. ClientPolicy.Tls.Enforce es falso.

Identificador: APPMESH_VIRTUAL_GATEWAY_BACKEND_DEFAULTS_TLS

Tipos de recursos: AWS::AppMesh::VirtualGateway

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appmesh-virtual-gateway-logging-file-path-exists

Comprueba si las puertas de enlace virtuales de AWS App Mesh tienen una ruta de archivo en la que escribir los registros de acceso. La regla no es compatible si es Configuration.spec.Logging. AccessLog.File.Path no existe.

Identificador: APPMESH_VIRTUAL_GATEWAY_LOGGING_FILE_PATH_EXISTS

Tipos de recursos: AWS::AppMesh::VirtualGateway

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appmesh-virtual-gateway-tagged

Comprueba si las pasarelas virtuales de AWS App Mesh tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves

de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPMESH_VIRTUAL_GATEWAY_TAGGED

Tipos de recursos: AWS::AppMesh::VirtualGateway

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appmesh-virtual-node-backend-defaults-tls-on

Comprueba si los valores predeterminados del backend de los nodos virtuales de AWS App Mesh requieren que los nodos virtuales se comuniquen con todos los puertos mediante TLS. La regla no cumple con los requisitos de Configuration.spec. BackendDefaults. ClientPolicy.Tls.Enforce es falso.

Identificador: APPMESH_VIRTUAL_NODE_BACKEND_DEFAULTS_TLS_ON

Tipos de recursos: AWS::AppMesh::VirtualNode

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appmesh-virtual-node-cloud-map-ip-pref-check

Comprueba si un nodo virtual de AWS App Mesh está configurado con la preferencia de IP especificada para AWS la detección del servicio Cloud Map. La regla es NON_COMPLIANT si el nodo virtual no está configurado con la preferencia de IP especificada en el parámetro de regla requerido.

Identificador: APPMESH_VIRTUAL_NODE_CLOUD_MAP_IP_PREF_CHECK

Tipos de recursos: AWS::AppMesh::VirtualNode

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

ipPreference, Tipo: cadena

El valor de preferencia de IP para AWS la detección del servicio Cloud Map. La regla es NON_COMPLIANT si un nodo virtual está configurado con un valor que no coincide con este

valor. Los valores válidos incluyen: 'IPv6_PREFERRED',' _PREFERRED', 'IPv4_ONLY' y' _ONLY'. IPv4 IPv6

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appmesh-virtual-node-dns-ip-pref-check

Comprueba si un nodo virtual de AWS App Mesh está configurado con la preferencia de IP especificada para la detección del servicio DNS. La regla es NON_COMPLIANT si el nodo virtual no está configurado con la preferencia de IP especificada en el parámetro de regla requerido.

Identificador: APPMESH_VIRTUAL_NODE_DNS_IP_PREF_CHECK

Tipos de recursos: AWS::AppMesh::VirtualNode

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

ipPreference, Tipo: cadena

El valor de preferencia de IP para detección de servicios de DNS. La regla es NON_COMPLIANT si un nodo virtual está configurado con un valor que no coincide con este valor. Los valores válidos incluyen: 'IPv6_PREFERRED',' IPv4 _PREFERRED', 'IPv4_ONLY' y' IPv6 _ONLY'.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appmesh-virtual-node-logging-file-path-exists

Comprueba si los nodos virtuales de AWS App Mesh tienen una ruta de archivo en la que escribir los registros de acceso. La regla no es compatible si es Configuration.spec.Logging. AccessLog.File.Path no existe.

Identificador: APPMESH_VIRTUAL_NODE_LOGGING_FILE_PATH_EXISTS

Tipos de recursos: AWS::AppMesh::VirtualNode

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appmesh-virtual-node-tagged

Comprueba si los nodos virtuales de AWS App Mesh tienen etiquetas. También puede especificar claves de etiqueta para comprobar la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPMESH_VIRTUAL_NODE_TAGGED

Tipos de recursos: AWS::AppMesh::VirtualNode

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appmesh-virtual-router-tagged

Comprueba si los routers virtuales AWS App Mesh tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPMESH_VIRTUAL_ROUTER_TAGGED

Tipos de recursos: AWS::AppMesh::VirtualRouter

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appmesh-virtual-service-tagged

Comprueba si los servicios virtuales de AWS App Mesh tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPMESH_VIRTUAL_SERVICE_TAGGED

Tipos de recursos: AWS::AppMesh::VirtualService

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)) Región

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

approved-amis-by-id

Comprueba si EC2 las instancias utilizan Amazon Machine Images (AMIs) especificadas. Especifique una lista de AMI aprobadas IDs. Las instancias en ejecución AMIs que no estén en esta lista no son conformes.

Identificador: APPROVED_AMIS_BY_ID

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

amiIds, Tipo: CSV

Lista separada por comas de hasta 21 AMI. IDs Hay un límite de 1024 caracteres.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

approved-amis-by-tag

Comprueba si EC2 las instancias utilizan Amazon Machine Images (AMIs) especificadas. Especifique las etiquetas que identifican el AMIs. Las instancias en ejecución AMIs que no tienen al menos una de las etiquetas especificadas son NON_COMPLIANT.

Identificador: APPROVED_AMIS_BY_TAG

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

amisByTagKeyAndValue, Tipo: StringMap, Predeterminado: tag-key:tag-value, other-tag-key

Lista de hasta 10 etiquetas separadas por comas (tag-key:tag-value). AMIs Por ejemplo, tag-key1 coincide con tag-key1; tag-key2:value2 coincide con tag-key2 con AMIs el valor 2.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

apprunner-service-in-vpc

Comprueba si los servicios de AWS App Runner enrutan el tráfico de salida a través de una VPC personalizada. La regla no cumple con las normas si está configurada. NetworkConfiguration. EgressConfiguration. EgressType es igual a DEFAULT.

Identificador: APPRUNNER_SERVICE_IN_VPC

Tipos de recursos: AWS::AppRunner::Service

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

apprunner-service-ip-address-verificación de tipo

Comprueba si un servicio de AWS App Runner está configurado con el tipo de dirección IP especificado para la configuración de la red pública entrante. La regla es NON_COMPLIANT si el servicio no está configurado con el tipo de dirección IP especificado en el parámetro de regla requerido.

Identificador: APPRUNNER_SERVICE_IP_ADDRESS_TYPE_CHECK

Tipos de recursos: AWS::AppRunner::Service

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

ipAddressType, Tipo: cadena

> El valor del tipo de dirección IP que la regla debe comprobar. La regla no es compatible si un servicio de AWS App Runner está configurado con un valor que no coincide con este valor. Los valores válidos incluyen: '', IPV4 'DUAL_STACK'.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

apprunner-service-max-unhealthy-umbral

Comprueba si un servicio de AWS App Runner está configurado para tener un umbral de mal estado inferior o igual al valor especificado. La regla es NON_COMPLIANT si el umbral de mal estado es mayor que el valor especificado en el parámetro de regla requerido.

Identificador: APPRUNNER_SERVICE_MAX_UNHEALTHY_THRESHOLD

Tipos de recursos: AWS::AppRunner::Service

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

maxUnhealthyThreshold, Tipo: int

> El valor máximo del umbral de mal estado que debe comprobar la regla. La regla no es compatible si un servicio de AWS App Runner está configurado con un umbral de mal estado superior a este valor. Los valores válidos son de 1 a 5.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

apprunner-service-no-public-acceso

Comprueba si AWS AppRunner los Servicios no son de acceso público. La regla no cumple con los requisitos de service.configuration. NetworkConfiguration. IngressConfiguration. IsPubliclyAccessible es falso.

Identificador: APPRUNNER_SERVICE_NO_PUBLIC_ACCESS

Tipos de recursos: AWS::AppRunner::Service

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

apprunner-service-observability-enabled

Comprueba si los servicios de AWS App Runner tienen habilitada la observabilidad. La regla NO ES COMPATIBLE si está configurada. ObservabilityConfiguration. ObservabilityEnabled es «falso».

Identificador: APPRUNNER_SERVICE_OBSERVABILITY_ENABLED

Tipos de recursos: AWS::AppRunner::Service

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

apprunner-service-tagged

Comprueba si los servicios de AWS App Runner tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPRUNNER_SERVICE_TAGGED

Tipos de recursos: AWS::AppRunner::Service

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

apprunner-vpc-connector-tagged

Comprueba si los conectores de VPC de AWS App Runner tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APPRUNNER_VPC_CONNECTOR_TAGGED

Tipos de recursos: AWS::AppRunner::VpcConnector

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney).

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appstream-fleet-in-vpc

Comprueba si las flotas de Amazon AppStream 2.0 utilizan una Amazon Virtual Private Cloud (Amazon VPC). La regla no cumple con las normas si está configurada. VpcConfig no existe. La regla no comprueba flotas de Elastic.

Identificador: APPSTREAM_FLEET_IN_VPC

Tipos de recursos: AWS::AppStream::Fleet

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

appsync-associated-with-waf

Comprueba si AWS AppSync APIs están asociadas a las listas de control de acceso AWS WAFv2 web ()ACLs. La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.

Identificador: APPSYNC_ASSOCIATED_WITH_WAF

Tipos de recursos: AWS::AppSync::GraphQLApi

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), Región de Europa (Zúrich)

Parámetros:

wafWebAclARNs (Opcional), Tipo: CSV

> Lista de nombres de recursos de Amazon (ARNs) separados por comas para sitios web autorizados. ACLs

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appsync-authorization-check

Comprueba si una AWS AppSync API utiliza los mecanismos de autorización permitidos. La regla es NON_COMPLIANT si se utiliza un mecanismo de autorización no aprobado.

Identificador: APPSYNC_AUTHORIZATION_CHECK

Tipos de recursos: AWS::AppSync::GraphQLApi

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

AllowedAuthorizationTypes, Tipo: CSV

> Lista de mecanismos de autorización permitidos separados por comas. AWS AppSync Los valores permitidos son: '', 'AWS_LAMBDA',API_KEY'AWS_IAM', 'OPENID_CONNECT', 'AMAZON_COGNITO_USER_POOLS'.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appsync-cache-ct-encryption-en reposo

Comprueba si la caché de una AWS AppSync API tiene activado el cifrado en reposo. Esta regla NO CUMPLE CON LOS REQUISITOS si 'AtRestEncryptionEnabled' es falso.

Identificador: APPSYNC_CACHE_CT_ENCRYPTION_AT_REST

Tipos de recursos: AWS::AppSync::ApiCache

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Medio Oriente (Baréin), Europa (Fráncfort), América del Sur (São Paulo) y Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appsync-cache-ct-encryption-en tránsito

Comprueba si la caché de una AWS AppSync API tiene activado el cifrado en tránsito. La regla no cumple con los requisitos si 'TransitEncryptionEnabled' es falso.

Identificador: APPSYNC_CACHE_CT_ENCRYPTION_IN_TRANSIT

Tipos de recursos: AWS::AppSync::ApiCache

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Medio Oriente (Baréin), Europa (Fráncfort), América del Sur (São Paulo) y Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appsync-cache-encryption-at-descanso

Comprueba si la caché de una AWS AppSync API tiene activado el cifrado en reposo. Esta regla NO CUMPLE CON LOS REQUISITOS si 'AtRestEncryptionEnabled' es falso.

Identificador: APPSYNC_CACHE_ENCRYPTION_AT_REST

Tipos de recursos: AWS::AppSync::GraphQLApi

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico

(Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appsync-graphql-api-xray-habilitado

Comprueba si AWS AppSync GraphQL tiene activado el rastreo de APIs AWS rayos X. La regla NO CUMPLE CON LOS REQUISITOS si está configurada. XrayEnabled es falsa.

Identificador: APPSYNC_GRAPHQL_ _ENABLED API_XRAY

Tipos de recursos: AWS::AppSync::GraphQLApi

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

appsync-logging-enabled

Comprueba si una AWS AppSync API tiene habilitado el registro a nivel de campo. La regla no cumple con los requisitos si el registro a nivel de campo no está habilitado o si los niveles de

registro de campos de la AppSync API no coinciden con los valores especificados en el parámetro «`fieldLoggingLevel`».

Identificador: APPSYNC_LOGGING_ENABLED

Tipos de recursos: AWS::AppSync::GraphQLApi

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

fieldLoggingLevel (Opcional), Tipo: CSV

> Lista separada por comas de niveles de registro de campo que la regla debe comprobar. Por ejemplo, “ERROR, INFO”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

aps-rule-groups-namespace-etiquetado

Comprueba si los espacios de nombres de grupos de reglas de Amazon Managed Service para Prometheus tienen etiquetas. Puede especificar las claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: APS_RULE_GROUPS_NAMESPACE_TAGGED

Tipos de recursos: AWS::APS::RuleGroupsNamespace

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), América del Sur (São

Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

athena-data-catalog-description

Comprueba si los catálogos de datos de Amazon Athena tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe.

Identificador: ATHENA_DATA_CATALOG_DESCRIPTION

Tipos de recursos: AWS::Athena::DataCatalog

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

athena-prepared-statement-description

Comprueba si las declaraciones preparadas de Amazon Athena tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe.

Identificador: ATHENA_PREPARED_STATEMENT_DESCRIPTION

Tipos de recursos: AWS::Athena::PreparedStatement

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Europa (Milán), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi) y China (Ningxia) región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

athena-workgroup-description

Comprueba si los grupos de trabajo de Amazon Athena tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: ATHENA_WORKGROUP_DESCRIPTION

Tipos de recursos: AWS::Athena::WorkGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

athena-workgroup-encrypted-at-descanso

Comprueba si un grupo de trabajo de Amazon Athena está cifrado en reposo. La regla es NON_COMPLIANT si el cifrado de datos en reposo no está habilitado para un grupo de trabajo de Athena.

Identificador: ATHENA_WORKGROUP_ENCRYPTED_AT_REST

Tipos de recursos: AWS::Athena::WorkGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

athena-workgroup-enforce-workgroup-configuración

Comprueba si los grupos de trabajo de Amazon Athena que utilizan el motor de Athena imponen la configuración de grupos de trabajo para anular la configuración del cliente. La regla no cumple con las normas si está configurada. WorkGroupConfiguration. EnforceWorkGroupConfiguration es falso.

Identificador: ATHENA_WORKGROUP_ENFORCE_WORKGROUP_CONFIGURATION

Tipos de recursos: AWS::Athena::WorkGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

athena-workgroup-engine-version-actualización automática

Comprueba si los grupos de trabajo de Amazon Athena que utilizan el motor Athena están configurados para actualización automática. La regla no cumple con las normas si está configurada. WorkGroupConfiguration. EngineVersion. SelectedEngineVersion no es «AUTOMÁTICO».

Identificador: ATHENA_WORKGROUP_ENGINE_VERSION_AUTO_UPGRADE

Tipos de recursos: AWS::Athena::WorkGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

athena-workgroup-logging-enabled

Comprueba si Amazon Athena WorkGroup publica métricas de uso en Amazon. CloudWatch La regla no cumple con los requisitos si Amazon WorkGroup Athena tiene el valor PublishCloudWatchMetricsEnabled «false».

Identificador: ATHENA_WORKGROUP_LOGGING_ENABLED

Tipos de recursos: AWS::Athena::WorkGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

auditmanager-assessment-tagged

Comprueba si las evaluaciones de AWS Audit Manager tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: AUDITMANAGER_ASSESSMENT_TAGGED

Tipos de recursos: AWS::AuditManager::Assessment

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

aurora-global-database-encryption-en reposo

Comprueba si las bases de datos globales de Amazon Aurora tienen activado el cifrado de almacenamiento. Esta regla NO CUMPLE CON LOS REQUISITOS si una base de datos global de Amazon Aurora no tiene activado el cifrado de almacenamiento.

Identificador: AURORA_GLOBAL_DATABASE_ENCRYPTION_AT_REST

Tipos de recursos: AWS::RDS::GlobalCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

aurora-last-backup-recovery-punto creado

Comprueba si se ha creado un punto de recuperación para los clústeres de bases de datos de Amazon Aurora. La regla es NON_COMPLIANT si el clúster de base de datos de Amazon Relational Database Service (Amazon RDS) no tiene un punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los clústeres de bases de datos de Aurora para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID del clúster de base de datos de Aurora que debe comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

aurora-meets-restore-time-objetivo

Comprueba si el tiempo de restauración de los clústeres de base de datos de Amazon Aurora cumple con la duración especificada. La regla no cumple con los requisitos si un clúster LatestRestoreExecutionTimeMinutes de base de datos Aurora es superior maxRestoreTime a minutos.

Identificador: AURORA_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

maxRestoreTime, Tipo: int

Valor numérico del tiempo de ejecución de restauración máximo permitido.

resourceTags (opcional), Tipo: cadena

Etiquetas de los clústeres de base de datos de Aurora para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID del clúster de base de datos de Aurora que debe comprobar la regla.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

aurora-mysql-backtracking-enabled

Comprueba si un clúster de Amazon Aurora MySQL tiene habilitada la función de retroceso. La regla es NON_COMPLIANT si el clúster de Aurora usa MySQL y no tiene habilitada la función de retroceso.

Identificador: AURORA_MYSQL_BACKTRACKING_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Solo disponible en Asia Pacífico (Bombay), Europa (París), EE.UU. Este (Ohio), Europa (Irlanda), Europa (Fráncfort), EE.UU. Este (Norte de Virginia), Asia Pacífico (Seúl), Asia Pacífico (Osaka), Europa (Londres), Asia Pacífico (Tokio), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Canadá (Región (Central)

Parámetros:

BacktrackWindowInHours (opcional), Tipo: double

> Cantidad de tiempo en horas (hasta 72) para realizar un seguimiento de su clúster de Aurora MySQL.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

aurora-mysql-cluster-audit-registro

Este control comprueba si los clústeres de MySQL DB de Amazon Aurora tienen habilitado el registro de auditoría. La regla es NON_COMPLIANT si un clúster de DB no tiene habilitado el registro de auditoría.

Identificador: AURORA_MYSQL_CLUSTER_AUDIT_LOGGING

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

aurora-resources-in-logically-air-gapped-vault

Comprueba si los clústeres de bases de datos de Amazon Aurora están en un almacén aislado lógicamente. La regla es NON_COMPLIANT si hay un clúster de base de datos de Amazon Aurora que no está en un almacén aislado lógicamente dentro del período de tiempo especificado.

Identificador: AURORA_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los clústeres de base de datos de Aurora para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID del clúster de base de datos de Aurora que debe comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 2184 horas y 91 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

aurora-resources-protected-by-plan de respaldo

Comprueba si los clústeres de bases de datos de Amazon Aurora están protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el clúster de bases de datos de Amazon Relational Database Service (Amazon RDS) no está protegido por un plan de copia de seguridad.

Identificador: AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los clústeres de bases de datos de Aurora para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID del clúster de base de datos de Aurora que debe comprobar la regla.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

autoscaling-capacity-rebalancing

Comprueba si el reequilibrio de capacidad está activado para los grupos de Amazon EC2 Auto Scaling que utilizan varios tipos de instancias. La regla es NON_COMPLIANT si Reequilibrio de la capacidad no está habilitado.

Identificador: AUTOSCALING_CAPACITY_REBALANCING

Tipos de recursos: AWS::AutoScaling::AutoScalingGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

autoscaling-group-elb-healthcheck-obligatorio

Comprueba si los grupos de Amazon EC2 Auto Scaling que están asociados a un Elastic Load Balancer utilizan comprobaciones de estado de Elastic Load Balancing. La regla no es conforme si los grupos de Amazon EC2 Auto Scaling no utilizan las comprobaciones de estado de Elastic Load Balancing.

Identificador: AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

Tipos de recursos: AWS::AutoScaling::AutoScalingGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con reglas. AWS Config Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-
balancer-3, ...]",
```

```
   "HealthCheckType": HealthCheckType*"
}
...
```

*Los valores válidos son `EC2` (predeterminado), `ELB` y `VPC_LATTICE`. El tipo de comprobación de estado `VPC_LATTICE` está reservado para utilizarse con VPC Lattice, que se encuentra en versión preliminar y está sujeto a cambios. Para obtener más información, consulte Comprobaciones de estado de las instancias de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

autoscaling-launchconfig-requires-imdsv2.

Comprueba si solo IMDSv2 está activado. Esta regla es NON_COMPLIANT si la versión de metadatos no está incluida en la configuración de lanzamiento o si los metadatos V1 y V2 están habilitados.

Identificador: AUTOSCALING_LAUNCHCONFIG_REQUIRES_ IMDSV2

Tipos de recursos: AWS::AutoScaling::LaunchConfiguration

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

autoscaling-launch-config-hop-límite

Comprueba el número de saltos de red que puede recorrer el token de metadatos. Esta regla es NON_COMPLIANT si el límite de saltos de respuesta de los metadatos es superior a 1.

Identificador: AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

Tipos de recursos: AWS::AutoScaling::LaunchConfiguration

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

autoscaling-launch-config-public-ip deshabilitada

Comprueba si los grupos de Amazon EC2 Auto Scaling tienen direcciones IP públicas habilitadas mediante las configuraciones de lanzamiento. La regla es NON_COMPLIANT si la configuración de lanzamiento de un grupo de Amazon EC2 Auto Scaling se ha AssociatePublicIpAddress establecido en «true».

Identificador: AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

Tipos de recursos: AWS::AutoScaling::LaunchConfiguration

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

autoscaling-launch-template

Comprueba si se ha creado un grupo de Auto Scaling de Amazon Elastic Compute Cloud (EC2) a partir de una plantilla de EC2 lanzamiento. La regla no cumple con los requisitos si el grupo de escalado no se crea a partir de una plantilla de EC2 lanzamiento.

Identificador: AUTOSCALING_LAUNCH_TEMPLATE

Tipos de recursos: AWS::AutoScaling::AutoScalingGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

autoscaling-multiple-az

Comprueba si el grupo de escalado automático se extiende en varias zonas de disponibilidad. La regla es NON_COMPLIANT si el grupo de escalado automático no abarca varias zonas de disponibilidad.

Identificador: AUTOSCALING_MULTIPLE_AZ

Tipos de recursos: AWS::AutoScaling::AutoScalingGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

minAvailabilityZones (Opcional), Tipo: int

Número mínimo de zonas de disponibilidad esperadas.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

autoscaling-multiple-instance-types

Comprueba si un grupo de Amazon EC2 Auto Scaling utiliza varios tipos de instancias. La regla es NON_COMPLIANT si el grupo Amazon EC2 Auto Scaling solo tiene un tipo de instancia definido. Esta regla no evalúa tipos de instancia basados en atributos.

Identificador: AUTOSCALING_MULTIPLE_INSTANCE_TYPES

Tipos de recursos: AWS::AutoScaling::AutoScalingGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

backup-plan-min-frequency-and-min-retention-check

Comprueba si un plan de copia de seguridad tiene una regla de copia de seguridad que cumpla con la frecuencia y el período de retención requeridos. La regla es NON_COMPLIANT si los puntos de recuperación no se crean al menos con la frecuencia especificada o si caducan antes del período especificado.

Identificador: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

Tipos de recursos: AWS::Backup::BackupPlan

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

requiredFrequencyValue (Opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la frecuencia de copia de seguridad requerida. Máximo de 24 para las horas y 31 para los días.

requiredRetentionDays (Opcional), Tipo: int, Valor predeterminado: 35

El periodo de retención obligatorio en días.

requiredFrequencyUnit (Opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la frecuencia de copia de seguridad requerida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

backup-recovery-point-encrypted

Comprueba si se ha cifrado un punto de recuperación. La regla es NON_COMPLIANT si el punto de recuperación no está cifrado.

Identificador: BACKUP_RECOVERY_POINT_ENCRYPTED

Tipos de recursos: AWS::Backup::RecoveryPoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

backup-recovery-point-manual-eliminación-deshabilitada

Comprueba si un almacén de copias de seguridad tiene adjunta una política basada en recursos que impide la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

> **Note**
>
> Se requiere un comodín para **`"Resource"`** y **`"Principal"`** de la instrucción Deny
> La regla requiere que el `"Resource"` y la `"Principal"` de la sentencia Deny incluyan un comodín en la política de acceso al almacén. De lo contrario, la regla devuelve NON_COMPLIANT.

Identificador: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

Tipos de recursos: AWS::Backup::BackupVault

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

principalArnList (Opcional), Tipo: CSV

Lista de nombres de recursos de Amazon () de AWS Identity and Access Management (IAM) separados por comas para que la regla ARNs NO los compruebe.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

backup-recovery-point-minimum- control de retención

Comprueba que un punto de recuperación no caduque antes de que concluya el período especificado. La regla es NON_COMPLIANT si el punto de recuperación tiene un punto de retención antes del período de retención requerido.

Identificador: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

Tipos de recursos: AWS::Backup::RecoveryPoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

requiredRetentionDays (Opcional), Tipo: int, Valor predeterminado: 35

El periodo de retención obligatorio en días.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

batch-compute-environment-enabled

Comprueba si los entornos de procesamiento AWS por lotes están habilitados. La regla es NON_COMPLIANT si el estado de configuración es “DISABLED”.

Identificador: BATCH_COMPUTE_ENVIRONMENT_ENABLED

Tipos de recursos: AWS::Batch::ComputeEnvironment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

batch-compute-environment-managed

Comprueba si los entornos de procesamiento AWS por lotes están gestionados. La regla es NON_COMPLIANT si el tipo de configuración .type es “UNMANAGED”.

Identificador: BATCH_COMPUTE_ENVIRONMENT_MANAGED

Tipos de recursos: AWS::Batch::ComputeEnvironment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

batch-compute-environment-tagged

Comprueba si los entornos de procesamiento AWS por lotes tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: BATCH_COMPUTE_ENVIRONMENT_TAGGED

Tipos de recursos: AWS::Batch::ComputeEnvironment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

batch-job-queue-enabled

Comprueba si las colas de trabajos AWS por lotes están habilitadas. La regla es NON_COMPLIANT si el estado de configuración es “DISABLED”.

Identificador: BATCH_JOB_QUEUE_ENABLED

Tipos de recursos: AWS::Batch::JobQueue

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

batch-job-queue-tagged

Comprueba si las colas de trabajos de AWS Batch tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: BATCH_JOB_QUEUE_TAGGED

Tipos de recursos: AWS::Batch::JobQueue

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

batch-managed-compute-environment-using-launch-template

Comprueba si los entornos de procesamiento gestionados AWS por Batch están configurados mediante una plantilla de lanzamiento. La regla no cumple con los requisitos si está configurada. ComputeResources. LaunchTemplate no existe.

Identificador: BATCH_MANAGED_COMPUTE_ENVIRONMENT_USING_LAUNCH_TEMPLATE

Tipos de recursos: AWS::Batch::ComputeEnvironment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

batch-managed-compute-env-allocation-strategy-check

Comprueba si un entorno informático gestionado AWS por lotes está configurado con una estrategia de asignación específica. La regla es NON_COMPLIANT si el entorno de computación no está configurado con una estrategia de asignación especificada en el parámetro de regla requerido.

Identificador: BATCH_MANAGED_COMPUTE_ENV_ALLOCATION_STRATEGY_CHECK

Tipos de recursos: AWS::Batch::ComputeEnvironment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

allocationStrategy, Tipo: CSV

> Lista separada por comas de estrategias de asignación que la regla debe comprobar. Los valores válidos son: “BEST_FIT”, “BEST_FIT_PROGRESSIVE”, “SPOT_CAPACITY_OPTIMIZED” y “SPOT_PRICE_CAPACITY_OPTIMIZED”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

batch-managed-compute-env-compute-resources-tagged

Comprueba si los recursos informáticos de los entornos informáticos gestionados por AWS lotes tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. Las etiquetas que comienzan por “aws:” no se comprueban.

Identificador: BATCH_MANAGED_COMPUTE_ENV_COMPUTE_RESOURCES_TAGGED

Tipos de recursos: AWS::Batch::ComputeEnvironment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

batch-managed-spot-compute-environment-max-bid

Comprueba si un entorno de cómputo puntual gestionado por AWS lotes está configurado para tener un porcentaje de oferta inferior o igual al valor especificado. La regla es NON_COMPLIANT si el porcentaje de oferta es mayor que el valor especificado en el parámetro de regla requerido.

Identificador: BATCH_MANAGED_SPOT_COMPUTE_ENVIRONMENT_MAX_BID

Tipos de recursos: AWS::Batch::ComputeEnvironment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud ,

(EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

maxBidPercentage, Tipo: int

El valor máximo del porcentaje de oferta que la regla debe comprobar. La regla no es compatible si un entorno de cómputo puntual gestionado AWS por lotes está configurado con un porcentaje de oferta superior a este valor. Los valores válidos están comprendidos entre 1 y 100.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

batch-scheduling-policy-tagged

Comprueba si las políticas de programación de AWS Batch tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: BATCH_SCHEDULING_POLICY_TAGGED

Tipos de recursos: AWS::Batch::SchedulingPolicy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

beanstalk-enhanced-health-reporting-habilitado

Comprueba si el entorno de AWS Elastic Beanstalk está configurado para mejorar los informes de estado. La regla es COMPLIANT si el entorno está configurado para informes de estado mejorados. La regla es NON_COMPLIANT si el entorno está configurado para informes de estado básicos.

Identificador: BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

Tipos de recursos: AWS::ElasticBeanstalk::Environment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México AWS GovCloud (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cassandra-keyspace-tagged

Comprueba si los Amazon Keyspaces (para Apache Cassandra) tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: CASSANDRA_KEYSPACE_TAGGED

Tipos de recursos: AWS::Cassandra::Keyspace

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Medio Oriente (Baréin), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Asia-Pacífico (Hong Kong), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Europa (Milán), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

clb-desync-mode-check

Comprueba si los equilibradores de carga clásicos (CLB) están configurados con un modo de mitigación de desincronización definido por el usuario. La regla es NON_COMPLIANT si el modo de mitigación de desincronización de CLB no coincide con el modo de mitigación de desincronización definido por el usuario.

Identificador: CLB_DESYNC_MODE_CHECK

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

desyncMode, Tipo: CSV

Lista separada por comas de los valores. Puede seleccionar un máximo de dos. Los valores válidos pueden ser los siguientes: defensivo, más estricto y supervisión.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

clb-multiple-az

Comprueba si un Classic Load Balancer abarca varias zonas de disponibilidad (). AZs La regla no es compatible si un Classic Load Balancer abarca menos de AZs 2 o no abarca el número AZs mencionado en `minAvailabilityZones` el parámetro (si se proporciona).

Identificador: CLB_MULTIPLE_AZ

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

minAvailabilityZones (Opcional), Tipo: int

Número mínimo deseado de expectativas AZs. Los valores válidos están entre 2 y 10, ambos inclusive. El valor predeterminado es 2 si no se especifica ningún parámetro.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudformation-stack-drift-detection-comprobar

Comprueba si la configuración real de una pila AWS CloudFormation (CloudFormation) es diferente o se ha desviado de la configuración esperada. Se considera que una pila se ha desviado si uno o varios de sus recursos difiere de su configuración esperada. La regla y la pila son COMPLIANT cuando el estado de desviación de la pila es IN_SYNC. La regla es NON_COMPLIANT si el estado de desviación de la pila es DRIFTED.

> **Note**
>
> Esta regla realiza la DetectStackDrift operación en cada pila de tu cuenta. La DetectStackDrift operación puede tardar varios minutos, según la cantidad de recursos que contenga la pila. Dado que el tiempo máximo de ejecución de esta regla está limitado a 15 minutos, es posible que se agote el tiempo de espera de la regla antes de completar la evaluación de todas las pilas de la cuenta.
> Si te encuentras con este problema, te recomendamos que restrinjas el número de pilas incluidas en el ámbito de aplicación de la regla mediante etiquetas. Se puede hacer lo siguiente:
>
> 1. Dividir las pilas en grupos, cada uno con una etiqueta diferente.
> 2. Aplicar la misma etiqueta a todas las pilas de ese grupo.
> 3. Tener varias instancias de esta regla en la cuenta, cada una con una etiqueta diferente. Esto permite que cada instancia de la regla procese solo las pilas que tengan la etiqueta correspondiente mencionada en su ámbito.

Identificador: CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

Tipos de recursos: AWS::CloudFormation::Stack

Tipo de desencadenador: cambios de configuración y periódicos

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Melbourne), Israel (Tel Aviv), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

cloudformationRoleArn, Tipo: cadena

El nombre de recurso de Amazon (ARN) de la función de IAM con permisos de política para detectar la desviación de las pilas. CloudFormation Para obtener más información sobre los permisos de IAM necesarios para el rol, consulte Detectar cambios de configuración no administrados en pilas y recursos con detección de derivación | Consideraciones a tener en cuenta cuando se detectan desviaciones en la Guía del usuario de CloudFormation .

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudformation-stack-notification-check

Comprueba si tus CloudFormation stacks envían notificaciones de eventos a un tema de Amazon SNS. Opcionalmente, comprueba si se están utilizando los temas de Amazon SNS especificados. La regla no cumple con los requisitos si las CloudFormation pilas no envían notificaciones.

Identificador: CLOUDFORMATION_STACK_NOTIFICATION_CHECK

Tipos de recursos: AWS::CloudFormation::Stack

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

snsTopic2 (opcional), Tipo: cadena

Tema de SNS: ARN.

snsTopic1 (opcional), Tipo: cadena

Tema de SNS: ARN.

snsTopic5 (opcional), Tipo: cadena

Tema de SNS: ARN.

snsTopic4 (opcional), Tipo: cadena

Tema de SNS: ARN.

snsTopic3 (opcional), Tipo: cadena

Tema de SNS: ARN.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudformation-stack-service-role-comprobar

Comprueba si las AWS CloudFormation pilas utilizan roles de servicio. La regla no es compatible si una CloudFormation pila no tiene una función de servicio asociada.

Identificador: CLOUDFORMATION_STACK_SERVICE_ROLE_CHECK

Tipos de recursos: AWS::CloudFormation::Stack

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudformation-termination-protection-check

Comprueba si una AWS CloudFormation pila tiene habilitada la protección de terminación. Esta regla NO CUMPLE CON LOS REQUISITOS si la protección de terminación no está habilitada en una CloudFormation pila.

Identificador: CLOUDFORMATION_TERMINATION_PROTECTION_CHECK

Tipos de recursos: AWS::CloudFormation::Stack

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cloudfront-accesslogs-enabled

Comprueba si CloudFront las distribuciones de Amazon están configuradas para entregar los registros de acceso a un bucket de Amazon S3 mediante el registro estándar (heredado). La regla no cumple con los requisitos si una CloudFront distribución no tiene configurado el registro heredado.

Identificador: CLOUDFRONT_ACCESSLOGS_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

S3 BucketName (opcional), Tipo: cadena

El nombre del bucket de Amazon S3 para almacenar los registros de acceso al servidor

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-associated-with-waf

Comprueba si CloudFront las distribuciones de Amazon están asociadas al firewall de aplicaciones web (WAF) o a las listas de control de acceso WAFv2 web (ACLs). La regla no cumple con los requisitos si una CloudFront distribución no está asociada a una ACL web de WAF.

Identificador: CLOUDFRONT_ASSOCIATED_WITH_WAF

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

wafWebAclIdentificadores (opcionales), Tipo: CSV

Lista separada por comas de ACL web IDs para WAF o ACL web Amazon Resource Names () para ARNs WAFV2

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-custom-ssl-certificate

Comprueba si el certificado asociado a una CloudFront distribución de Amazon es el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

Identificador: CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-default-root-object-configurado

Comprueba si una CloudFront distribución de Amazon está configurada para devolver un objeto específico que es el objeto raíz predeterminado. La regla es NON_COMPLIANT si la CloudFront distribución de Amazon no tiene configurado un objeto raíz predeterminado.

Identificador: CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-distribution-key-group-habilitado

Comprueba si CloudFront las distribuciones de Amazon están configuradas para usar solo grupos de claves de confianza para la autenticación de URL o cookies firmadas para todos los comportamientos de la caché. La regla no cumple con los requisitos si algún comportamiento de caché de la distribución utiliza firmantes de confianza.

Identificador: CLOUDFRONT_DISTRIBUTION_KEY_GROUP_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cloudfront-no-deprecated-ssl-protocolos

Comprueba si CloudFront las distribuciones utilizan protocolos SSL obsoletos para la comunicación HTTPS entre ubicaciones de CloudFront borde y orígenes personalizados. Esta regla no cumple con las condiciones de una CloudFront distribución si alguna de las distribuciones «incluyeOriginSslProtocols». SSLv3

Identificador: CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-origin-access-identity-habilitado

Comprueba si la CloudFront distribución con el tipo de origen de Amazon S3 tiene configurada la identidad de acceso de origen. La regla no cumple con los requisitos si la CloudFront distribución está respaldada por S3 y cualquier tipo de origen no está configurado para la OAI o si el origen no es un bucket de S3.

> **Note**
>
> La regla no devuelve `NOT_APPLICABLE` si el origen no es un bucket de S3.

Identificador: CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-origin-failover-enabled

Comprueba si un grupo de origen está configurado para la distribución de al menos dos orígenes en el grupo de origen de Amazon CloudFront. La regla es NON_COMPLIANT si no hay grupos de origen para la distribución.

Identificador: CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-origin-lambda-url-habilitado para oac

Comprueba si CloudFront las distribuciones de Amazon con orígenes de URL de la función Amazon Lambda tienen activado el control de acceso de origen (OAC). La regla es NON_COMPLIANT si alguna URL de origen de una función Lambda en una CloudFront distribución no tiene habilitada la OAC.

Identificador: CLOUDFRONT_ORIGIN_LAMBDA_URL_OAC_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

frente a nubos-s3- origin-access-control-enabled

Comprueba si una CloudFront distribución de Amazon con un tipo de origen Amazon Simple Storage Service (Amazon S3) tiene activado el control de acceso al origen (OAC). La regla es NON_COMPLIANT para CloudFront las distribuciones con orígenes de Amazon S3 que no tienen habilitada la OAC.

Identificador: CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

frente a nubos-s3- origin-non-existent-bucket

Comprueba si CloudFront las distribuciones de Amazon apuntan a un bucket de S3 inexistente. La regla no cumple con los requisitos si `S3 OriginConfig `de una CloudFront distribución apunta a un bucket de S3 que no existe. La regla no evalúa los depósitos de S3 con alojamiento de sitios web estáticos.

Identificador: CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: periódico

Región de AWS: solo está disponible en China (Pekín) y en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-security-policy-check

Comprueba si CloudFront las distribuciones de Amazon utilizan una política de seguridad mínima y un conjunto de cifrado de TLSv1 0,2 o superior para las conexiones de los espectadores. Esta regla NO CUMPLE con las condiciones de una CloudFront distribución si el valor es inferior a .2_2018. minimumProtocolVersion TLSv1

Identificador: CLOUDFRONT_SECURITY_POLICY_CHECK

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-sni-enabled

Comprueba si CloudFront las distribuciones de Amazon utilizan un certificado SSL personalizado y si están configuradas para utilizar el SNI para atender las solicitudes HTTPS. La regla es NON_COMPLIANT si se asocia un certificado SSL personalizado, pero el método de compatibilidad con SSL es una dirección IP dedicada.

Identificador: CLOUDFRONT_SNI_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-ssl-policy-check

Comprueba si CloudFront las distribuciones de Amazon están configuradas con las políticas de seguridad especificadas. La regla es NON_COMPLIANT si una CloudFront distribución no está configurada con las políticas de seguridad que especifiques.

Identificador: CLOUDFRONT_SSL_POLICY_CHECK

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

securityPolicies, Tipo: CSV

> Lista de políticas de seguridad de CloudFront distribución separadas por comas para que la regla las compruebe. Por ejemplo: "TLSv1.2_2018, .2_2019, .2_2021". TLSv1 TLSv1 Para obtener una lista de valores válidos, consulta la Guía para CloudFront desarrolladores de Amazon.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudfront-traffic-to-origin-encriptado

Comprueba si CloudFront las distribuciones de Amazon cifran el tráfico a orígenes personalizados. La regla no cumple con los requisitos si «» OriginProtocolPolicy es «solo para HTTP» o si «» es «visor de partidos» y «OriginProtocolPolicy» es «permitido todo». ViewerProtocolPolicy

Identificador: CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cloudfront-viewer-policy-https

Comprueba si tus CloudFront distribuciones de Amazon utilizan HTTPS (directamente o mediante una redirección). La regla no cumple con los requisitos si el valor de ViewerProtocolPolicy está establecido en 'allow-all' para el o para el. defaultCacheBehavior CacheBehaviors

Identificador: CLOUDFRONT_VIEWER_POLICY_HTTPS

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudtrail-all-read-s3- data-event-check

Comprueba si un registro AWS CloudTrail multirregional está activado y registra todos los eventos de datos de S3 leídos de tus buckets. La regla es NON_COMPLIANT si no hay ningún registro de seguimiento multirregional que registre todos los tipos de eventos de datos de S3 de lectura para todos los buckets de S3 actuales y futuros.

Identificador: CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudtrail-all-write-s3- data-event-check

Comprueba si un registro AWS CloudTrail multirregional está activado y registra todos los eventos de escritura de datos de S3 de tus buckets. La regla es NON_COMPLIANT si no hay ningún registro de seguimiento multirregional que registre todos los tipos de eventos de datos de S3 de escritura para todos los buckets de S3 actuales y futuros.

Identificador: CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rastro de nubes -S3- bucket-access-logging

Comprueba si las configuraciones del bucket de S3 para sus AWS CloudTrail registros tienen activado el registro de acceso al servidor Amazon S3. La regla no cumple con los requisitos si al menos un bucket de S3 para una CloudTrail ruta no tiene activado el registro de acceso al servidor S3.

Identificador: CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

Tipos de recursos: AWS::CloudTrail::Trail

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rastro de nubes -S3- bucket-public-access-prohibited

Comprueba si las configuraciones del bucket de S3 de sus AWS CloudTrail registros bloquean el acceso público. La regla no cumple con los requisitos si al menos un depósito de S3 para una CloudTrail ruta es de acceso público.

Identificador: CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROHIBITED

Tipos de recursos: AWS::CloudTrail::Trail

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cloudtrail-s3-dataevents-enabled

Comprueba si al menos un AWS CloudTrail rastro está registrando eventos de datos de Amazon Simple Storage Service (Amazon S3) para todos los buckets de S3. La regla es NON_COMPLIANT si hay registros de seguimiento o si no hay registros de seguimiento de los eventos de datos de S3.

Identificador: CLOUDTRAIL_S3_DATAEVENTS_ENABLED

Tipo de disparador: periódico

Región de AWS: Todas las regiones compatibles AWS

Parámetros:

S3 BucketNames (opcional), Tipo: cadena

> Lista separada por comas de nombres de bucket de S3 para los que se debe habilitar el registro de eventos de datos. Comprueba el comportamiento predeterminado de todos los buckets de S3.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudtrail-security-trail-enabled

Comprueba que haya al menos un AWS CloudTrail rastro definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimiento que cumpla todos los requisitos siguientes:

- registra eventos de servicios globales
- es un registro de seguimiento de varias regiones
- tiene habilitada la validación de archivos de registro
- está cifrado con una clave de KMS
- registra eventos para lecturas y escrituras
- registra eventos de administración
- no excluye ningún evento de administración

Esta regla es NON_COMPLIANT si ningún registro de seguimiento cumple con todos los criterios mencionados anteriormente.

Identificador: CLOUDTRAIL_SECURITY_TRAIL_ENABLED

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudwatch-alarm-action-check

Comprueba si CloudWatch las alarmas tienen una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Opcionalmente, comprueba si alguna acción coincide con un ARN designado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

Identificador: CLOUDWATCH_ALARM_ACTION_CHECK

Tipos de recursos: AWS::CloudWatch::Alarm

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

okActionRequired, Tipo: cadena, Predeterminado: false

Las alarmas tienen al menos una acción cuando la alarma pasa a un estado OK desde cualquier otro estado.

insufficientDataActionNecesario, Tipo: cadena, Predeterminado: true

Las alarmas tienen al menos una acción cuando la alarma pasa al estado INSUFFICIENT_DATA desde cualquier otro estado.

alarmActionRequired, Tipo: cadena, Predeterminado: true

Las alarmas tienen al menos una acción.

action1 (opcional), Tipo: cadena

La acción que se va a ejecutar, especificada como un ARN.

action2 (opcional), Tipo: cadena

La acción que se va a ejecutar, especificada como un ARN.

action3 (opcional), Tipo: cadena

La acción que se va a ejecutar, especificada como un ARN.

action4 (opcional), Tipo: cadena

La acción que se va a ejecutar, especificada como un ARN.

action5 (opcional), Tipo: cadena

La acción que se va a ejecutar, especificada como un ARN.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudwatch-alarm-action-enabled-comprobar

Comprueba si CloudWatch las acciones de las alarmas de Amazon están activadas. La regla no cumple con los requisitos si las acciones de las CloudWatch alarmas no están activadas.

Identificador: CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

Tipos de recursos: AWS::CloudWatch::Alarm

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudwatch-alarm-resource-check

Comprueba si un tipo de recurso tiene una CloudWatch alarma para la métrica nombrada. Para el tipo de recurso, puede especificar volúmenes, EC2 instancias, clústeres de Amazon RDS o buckets S3 de EBS. La regla cumple con los requisitos si la métrica indicada tiene un identificador de recurso y una alarma. CloudWatch

Identificador: CLOUDWATCH_ALARM_RESOURCE_CHECK

Tipos de recursos: AWS::EC2::Instance, AWS::RDS::DBCluster, AWS::S3::Bucket, AWS::EC2::Volume

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

resourceType, Tipo: cadena

AWS tipo de recurso. El valor puede ser uno de los siguientes: AWS::EC2::Volume AWS::EC2::Instance, AWS::RDS::DBCluster, o AWS::S3::Bucket.

metricName, Tipo: cadena

El nombre de la métrica asociada a la alarma (por ejemplo, 'CPUUtilization' para EC2 las instancias).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cloudwatch-alarm-settings-check

Comprueba si CloudWatch las alarmas con el nombre de métrica indicado tienen la configuración especificada.

Identificador: CLOUDWATCH_ALARM_SETTINGS_CHECK

Tipos de recursos: AWS::CloudWatch::Alarm

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

metricName, Tipo: cadena

El nombre de la métrica asociada a la alarma.

period (opcional), Tipo: int, Valor predeterminado: 300

El periodo, en segundos, durante el cual se aplica la estadística especificada.

statistic (opcional), Tipo: cadena

Estadística de la métrica asociada a la alarma (por ejemplo, Average o Sum).

comparisonOperator (opcional), Tipo: cadena

La operación para comparar la estadística y el umbral especificados (por ejemplo, ''). GreaterThanThreshold

threshold (opcional), Tipo: int

El valor con el que se compara la estadística especificada.

evaluationPeriods (opcional), Tipo: int

El número de periodos en los que los datos se comparan con el umbral especificado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudwatch-log-group-encrypted

Comprueba si los grupos de CloudWatch registros de Amazon están cifrados con alguna clave de AWS KMS o con un identificador de clave de AWS KMS específico. La regla no cumple con los requisitos si un grupo de CloudWatch registros no se cifra con una clave de KMS o se cifra con una clave de KMS que no se proporciona en el parámetro de la regla.

Identificador: CLOUDWATCH_LOG_GROUP_ENCRYPTED

Tipos de recursos: AWS::Logs::LogGroup

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

KmsKeyId (Opcional), Tipo: cadena

Nombre de recurso de Amazon (ARN) del ID para la clave de KMS que se utiliza para cifrar el grupo de registro.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloudwatch-metric-stream-tagged

Comprueba si las transmisiones CloudWatch métricas de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: CLOUDWATCH_METRIC_STREAM_TAGGED

Tipos de recursos: AWS::CloudWatch::MetricStream

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloud-trail-cloud-watch-registros habilitados

Comprueba si los AWS CloudTrail senderos están configurados para enviar registros a CloudWatch registros. El sendero NO CUMPLE CON LAS NORMAS si la CloudWatchLogsLogGroupArn propiedad del sendero está vacía.

Identificador: CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

Tipos de recursos: AWS::CloudTrail::Trail

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

expectedDeliveryWindowEdad (opcional), Tipo: int

> Antigüedad máxima en horas desde la entrega más reciente de los CloudWatch registros que cumplan con la normativa.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cloudtrail-enabled

> **Important**
>
> Para esta regla, el identificador de la regla (CLOUD_TRAIL_ENABLED) y el nombre de la regla (cloudtrail-enabled) son diferentes.

Comprueba si hay una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimiento habilitado. Opcionalmente, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

Identificador: CLOUD_TRAIL_ENABLED

Tipo de disparador: periódico

Región de AWS: todas las regiones compatibles AWS

Parámetros:

s3 BucketName (opcional), Tipo: cadena

Nombre del depósito de S3 CloudTrail al que se van a entregar los archivos de registro.

snsTopicArn (Opcional), Tipo: cadena

El ARN del tema de SNS CloudTrail para usarlo en las notificaciones.

cloudWatchLogsLogGroupArn (Opcional), Tipo: cadena

CloudWatch ARN del grupo de registros CloudTrail al que enviar datos.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cloud-trail-encryption-enabled

Comprueba si AWS CloudTrail está configurado para utilizar el cifrado del lado del servidor (SSE AWS KMS) AWS Key Management Service (). La regla cumple con las normas si KmsKeyId está definida.

Identificador: CLOUD_TRAIL_ENCRYPTION_ENABLED

Tipos de recursos: AWS::CloudTrail::Trail

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cloud-trail-log-file-habilitada para validación

Comprueba si AWS CloudTrail crea un archivo de resumen firmado con registros. AWS recomienda que la validación de archivos esté habilitada en todos los senderos. La regla es NON_COMPLIANT si la validación no se ha habilitado.

Identificador: CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

Tipos de recursos: AWS::CloudTrail::Trail

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cmk-backing-key-rotation-habilitado

Comprueba si la rotación automática de claves está habilitada para cada clave y si coincide con el ID de clave de la clave AWS KMS creada por el cliente. La regla es NON_COMPLIANT si el rol de grabador AWS Config de un recurso no tiene el kms: DescribeKey permiso.

> **Note**
>
> La rotación automática de claves no es compatible con las claves de KMS asimétricas, las claves de KMS HMAC, las claves de KMS con material de claves importado o las claves de KMS en almacenes de claves personalizados.

Identificador: CMK_BACKING_KEY_ROTATION_ENABLED

Tipos de recursos: AWS::KMS::Key

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

codebuild-project-artifact-encryption

Comprueba si un AWS CodeBuild proyecto tiene el cifrado activado para todos sus artefactos. La regla kms:DescribeKey si encryptionDisabled se establece en true para cualquier configuración de artefacto principal o secundario (si está presente).

Identificador: CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

Tipos de recursos: AWS::CodeBuild::Project

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

codebuild-project-environment-privileged-comprobar

Comprueba si el entorno de un proyecto tiene activado el modo privilegiado. AWS CodeBuild La regla es NON_COMPLIANT para un CodeBuild proyecto si 'PrivilegedMode' se establece en 'true'.

Identificador: CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

Tipos de recursos: AWS::CodeBuild::Project

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

exemptedProjects (opcional), Tipo: CSV

> Lista de nombres de CodeBuild proyectos separados por comas que pueden tener 'PrivilegedMode' con el valor 'true'.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

codebuild-project-envvar-awscred-comprobar

Comprueba si el proyecto contiene las variables de entorno _ACCESS_KEY_ID y _SECRET_ACCESS_KEY. AWS AWS La regla es NON_COMPLIANT si las variables de entorno del proyecto contienen credenciales de texto no cifrado.

Identificador: CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK

Tipos de recursos: AWS::CodeBuild::Project

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

codebuild-project-logging-enabled

Comprueba si un entorno de AWS CodeBuild proyecto tiene habilitada al menos una opción de registro. La regla es NON_COMPLIANT si el estado de todas las configuraciones de registro actuales está establecido en DISABLED.

Identificador: CODEBUILD_PROJECT_LOGGING_ENABLED

Tipos de recursos: AWS::CodeBuild::Project

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

s3 BucketNames (opcional), Tipo: cadena

Lista separada por comas de los nombres de los buckets de Amazon S3 a los que se deben enviar los registros si los registros de S3 están configurados.

cloudWatchGroupNombres (opcional), Tipo: cadena

Lista separada por comas de los nombres de los grupos de registros de Amazon CloudWatch a los que se deben enviar los CloudWatch registros si los registros están configurados.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

codebuild-project-sCifrado de 3 registros

Comprueba si un AWS CodeBuild proyecto configurado con Amazon S3 Logs tiene el cifrado activado para sus registros. La regla no es compatible si 'EncryptionDisabled' se establece en 'true' en el S3 LogsConfig de un proyecto. CodeBuild

Identificador: CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

Tipos de recursos: AWS::CodeBuild::Project

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

exemptedProjects (opcional), Tipo: CSV

> Lista de nombres de CodeBuild proyectos separados por comas que pueden generar registros sin cifrar.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

codebuild-project-source-repo-comprobación de URL

Comprueba si la URL del repositorio fuente de Bitbucket contiene credenciales de inicio de sesión o no. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.

Identificador: CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

Tipos de recursos: AWS::CodeBuild::Project

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

codebuild-report-group-encrypted-en reposo

Comprueba si un grupo de AWS CodeBuild informes tiene habilitada la configuración de cifrado en reposo. La regla no cumple con los requisitos si «» es «EncryptionDisabledverdadera».

Identificador: CODEBUILD_REPORT_GROUP_ENCRYPTED_AT_REST

Tipos de recursos: AWS::CodeBuild::ReportGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

codebuild-report-group-tagged

Comprueba si los grupos de AWS CodeBuild informes tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: CODEBUILD_REPORT_GROUP_TAGGED

Tipos de recursos: AWS::CodeBuild::ReportGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

codedeploy-auto-rollback-monitor-habilitado

Comprueba si el grupo de implementación está configurado con la reversión automática de la implementación y la supervisión de la implementación con alarmas asociadas. La regla no es compatible si no se AlarmConfiguration ha configurado AutoRollbackConfiguration o no está habilitada.

Identificador: CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

Tipos de recursos: AWS::CodeDeploy::DeploymentGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

codedeploy-deployment-group-auto-habilitado para la reversión

Comprueba si los grupos AWS CodeDeploy de despliegue tienen habilitada la configuración de reversión automática. La regla NO ES COMPATIBLE si está configurada. autoRollbackConfiguration.enabled es falso o no existe.

Identificador: CODEDEPLOY_DEPLOYMENT_GROUP_AUTO_ROLLBACK_ENABLED

Tipos de recursos: AWS::CodeDeploy::DeploymentGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

codedeploy-deployment-group-outdated-actualización de instancias

Comprueba si los grupos de AWS CodeDeploy despliegue actualizan automáticamente las instancias desactualizadas. La regla NO CUMPLE CON LOS REQUISITOS si está configurada. outdatedInstancesStrategy es «IGNORAR».

Identificador: CODEDEPLOY_DEPLOYMENT_GROUP_OUTDATED_INSTANCES_UPDATE

Tipos de recursos: AWS::CodeDeploy::DeploymentGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

código deploy-ec2- minimum-healthy-hosts-configured

Comprueba si el grupo de implementación de EC2 /On-Premises Compute Platform está configurado con un porcentaje mínimo de flota de hosts en buen estado o un número de hosts superior o igual al umbral de entrada. La regla es NON_COMPLIANT si alguno está por debajo del umbral.

Identificador: CODEDEPLOY_ _MINIMUM_HEALTHY_HOSTS_CONFIGURED EC2

Tipos de recursos: AWS::CodeDeploy::DeploymentGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

minimumHealthyHostsFleetPercent (Opcional), Tipo: int, Valor predeterminado: 66

Porcentaje mínimo de una flota de hosts en buen estado durante la implementación. El valor predeterminado es 66 %.

minimumHealthyHostsHostCount (Opcional), Tipo: int, Valor predeterminado: 1

Número mínimo de hosts en buen estado en la flota durante la implementación. El valor predeterminado es 1.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

codedeploy-lambda-allatonce-traffic-turno desactivado

Comprueba si el grupo de implementación de Lambda Compute Platform no utiliza la configuración de implementación predeterminada. La regla no es compatible si el grupo de despliegue utiliza la configuración de despliegue '. CodeDeployDefault LambdaAllAtOnce'.

Identificador: CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

Tipos de recursos: AWS::CodeDeploy::DeploymentGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

codeguruprofiler-profiling-group-tagged

Comprueba si los grupos de CodeGuru perfiles de Amazon Profiler tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: CODEGURUPROFILER_PROFILING_GROUP_TAGGED

Tipos de recursos: AWS::CodeGuruProfiler::ProfilingGroup

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

codegurureviewer-repository-association-tagged

Comprueba si las asociaciones de repositorios de Amazon CodeGuru Reviewer tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: CODEGURUREVIEWER_REPOSITORY_ASSOCIATION_TAGGED

Tipos de recursos: AWS::CodeGuruReviewer::RepositoryAssociation

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

codepipeline-deployment-count-check

Comprueba si la primera etapa de despliegue AWS CodePipeline realiza más de un despliegue. Opcionalmente, comprueba si cada una de las etapas restantes posteriores se implementa en más del número de implementaciones especificado (`deploymentLimit`).

Identificador: CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

Tipos de recursos: AWS::CodePipeline::Pipeline

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

deploymentLimit (opcional), Tipo: int

El número máximo de implementaciones que puede realizar cada etapa.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

codepipeline-region-fanout-check

Comprueba si cada etapa de la fase se AWS CodePipeline despliega en más de N veces el número de regiones que AWS CodePipeline ha desplegado en todas las fases combinadas anteriores, donde N es el número de regiones dispersas. La primera etapa de implementación puede implementar en un máximo de una región y la segunda etapa de implementación puede implementar en un número máximo especificado en `regionFanoutFactor`. Si no proporciona un `regionFanoutFactor`, el valor predeterminado es tres. Por ejemplo: Si la 1ª etapa de implementación implementa en una región y la 2ª etapa de implementación se implementa en tres regiones, la 3ª etapa de implementación puede implementar en 12 regiones, es decir, la suma de las etapas anteriores multiplicada por el número de distribuciones ramificadas de la región (tres). La regla es NON_COMPLIANT si la implementación está en más de una región en la 1ª etapa o tres regiones en la 2ª etapa o 12 regiones en la 3ª etapa.

Identificador: CODEPIPELINE_REGION_FANOUT_CHECK

Tipos de recursos: AWS::CodePipeline::Pipeline

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

regionFanoutFactor (Opcional), Tipo: int, Valor predeterminado: 3

> El número de regiones en las que se AWS CodePipeline ha desplegado en todas las etapas anteriores es el número aceptable de regiones en las que se puede desplegar cualquier etapa.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cognito-identity-pool-unauthenticated-inicios de sesión

Comprueba si los grupo de identidades de Amazon Cognito no permiten identidades no autenticadas. La regla no cumple con las normas si está configurada. AllowUnauthenticatedIdentities es cierto.

Identificador: COGNITO_IDENTITY_POOL_UNAUTHENTICATED_LOGINS

Tipos de recursos: AWS::Cognito::IdentityPool

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cognito-identity-pool-unauth-control de acceso

Comprueba si un grupo de identidades de Amazon Cognito permite identidades no autenticadas. La regla es NON_COMPLIANT si el grupo de identidades está configurado para permitir identidades no autenticadas.

Identificador: COGNITO_IDENTITY_POOL_UNAUTH_ACCESS_CHECK

Tipos de recursos: AWS::Cognito::IdentityPool

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia) AWS GovCloud , (EE. UU. Este), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cognito-userpool-cust-auth-threat-full-check

Comprueba si los grupos de usuarios de Amazon Cognito tienen habilitada la protección contra amenazas con un modo de aplicación de todas las funciones para la autenticación personalizada. Esta regla no cumple con los requisitos si la protección contra amenazas para la autenticación personalizada no está configurada en un modo de aplicación con todas las funciones.

Identificador: COGNITO_USERPOOL_CUST_AUTH_THREAT_FULL_CHECK

Tipos de recursos: AWS::Cognito::UserPool

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cognito-user-pool-advanced-con seguridad habilitada

Comprueba si un grupo de usuarios de Amazon Cognito tiene habilitada la seguridad avanzada para autenticación estándar. La regla es NON_COMPLIANT si la seguridad avanzada no está habilitada. Si lo desea, puede especificar un modo de seguridad avanzado que la regla debe comprobar.

Identificador: COGNITO_USER_POOL_ADVANCED_SECURITY_ENABLED

Tipos de recursos: AWS::Cognito::UserPool

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hong Kong), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

SecurityMode (Opcional), Tipo: cadena

> Valor de cadena del modo de seguridad avanzado que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el modo de seguridad avanzada de los grupos de usuarios no coincide con este valor del parámetro. Los valores válidos son AUDIT y ENFORCED

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cognito-user-pool-deletion-protección habilitada

Comprueba si los grupos de usuarios de Amazon Cognito tienen habilitada la protección contra la eliminación. Esta regla NO CUMPLE CON LOS REQUISITOS si un grupo de usuarios tiene deshabilitada la protección contra la eliminación.

Identificador: COGNITO_USER_POOL_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::Cognito::UserPool

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cognito-user-pool-mfa-habilitado

Comprueba si los grupos de usuarios de Amazon Cognito configurados con una política de inicio de sesión solo con contraseña tienen habilitada la Autenticación Multi-Factor (MFA). Esta regla NO ES COMPATIBLE si el grupo de usuarios de Cognito configurado con la política de inicio de sesión solo con CONTRASEÑA no tiene habilitada la MFA.

Identificador: COGNITO_USER_POOL_MFA_ENABLED

Tipos de recursos: AWS::Cognito::UserPool

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

cognito-user-pool-password-verificación de políticas

Comprueba si la política de contraseñas del grupo de usuarios de Amazon Cognito cumple los requisitos especificados que se indican en los parámetros. La regla es NON_COMPLIANT si la política de contraseñas del grupo de usuarios no cumple los requisitos especificados.

Identificador: COGNITO_USER_POOL_PASSWORD_POLICY_CHECK

Tipos de recursos: AWS::Cognito::UserPool

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requireSymbols (opcional), Tipo: booleano, Valor predeterminado: True

Requiere que al menos haya un símbolo en la contraseña.

temporaryPasswordValidity (Opcional), Tipo: int, Valor predeterminado: 7

Número de días que una contraseña temporal sigue siendo válida.

minLength (opcional), Tipo: int, Predeterminado: 8

Longitud mínima requerida para la contraseña del grupo de usuarios.

requireNumbers (opcional), Tipo: booleano, Valor predeterminado: True

Si se requiere que haya al menos un número en la contraseña.

requireUppercase (opcional), Tipo: booleano, Valor predeterminado: True

Si se requiere que haya al menos una letra mayúscula en la contraseña.

requireLowercase (opcional), Tipo: booleano, Valor predeterminado: True

Si se requiere que haya al menos una letra minúscula en la contraseña.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cognito-user-pool-tagged

Comprueba si los grupos de usuarios de Amazon Cognito tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: COGNITO_USER_POOL_TAGGED

Tipos de recursos: AWS::Cognito::UserPool

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

connect-instance-logging-enabled

Comprueba si las instancias de Amazon Connect tienen habilitados los registros de flujo en un grupo de CloudWatch registros de Amazon. La regla es NON_COMPLIANT si una instancia de Amazon Connect tiene habilitados flujos de registros.

Identificador: CONNECT_INSTANCE_LOGGING_ENABLED

Tipos de recursos: AWS::Connect::Instance

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en África (Ciudad del Cabo), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

customerprofiles-domain-tagged

Comprueba si los dominios de los perfiles de clientes de Amazon Connect tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: CUSTOMERPROFILES_DOMAIN_TAGGED

Tipos de recursos: AWS::CustomerProfiles::Domain

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en África (Ciudad del Cabo), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

customerprofiles-object-type-allow-creación de perfiles

Comprueba si los tipos de objetos de los perfiles de clientes de Amazon Connect permiten la creación de un nuevo perfil estándar si no existe ninguno. La regla no cumple con las normas si está configurada. AllowProfileCreation es falsa.

Identificador: CUSTOMERPROFILES_OBJECT_TYPE_ALLOW_PROFILE_CREATION

Tipos de recursos: AWS::CustomerProfiles::ObjectType

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en África (Ciudad del Cabo), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

customerprofiles-object-type-tagged

Comprueba si los tipos de objetos de Perfiles de clientes de Amazon Connect tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: CUSTOMERPROFILES_OBJECT_TYPE_TAGGED

Tipos de recursos: AWS::CustomerProfiles::ObjectType

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en África (Ciudad del Cabo), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

custom-eventbus-policy-attached

Comprueba si los autobuses de eventos EventBridge personalizados de Amazon tienen adjunta una política basada en recursos. La regla es NON_COMPLIANT si una política de bus de eventos personalizada no tiene una política asociada basada en recursos.

Identificador: CUSTOM_EVENTBUS_POLICY_ATTACHED

Tipos de recursos: AWS::Events::EventBus

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

custom-schema-registry-policy-adjunto

Comprueba si los registros de EventBridge esquemas personalizados de Amazon tienen una política de recursos adjunta. La regla es NON_COMPLIANT para los registros de esquemas personalizados sin una política de recursos adjunta.

Identificador: CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

Tipos de recursos: AWS::EventSchemas::Registry

Tipo de disparador: periódico

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Asia-Pacífico (Hong Kong), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

cw-loggroup-retention-period-comprobar

Comprueba si el período CloudWatch LogGroup de retención de Amazon está establecido en más de 365 días o si es un período de retención específico. La regla es NON_COMPLIANT si el período de retención es inferior a `MinRetentionTime` (si se ha especificado) o a 365 días.

> **Note**
>
> Si la configuración de retención es No caducará nunca para un grupo de registro, la regla se marcará como COMPLIANT.

Identificador: CW_LOGGROUP_RETENTION_PERIOD_CHECK

Tipos de recursos: AWS::Logs::LogGroup

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

LogGroupNames (Opcional), Tipo: CSV

Lista separada por comas de los nombres del grupo de registro para comprobar el periodo de retención.

MinRetentionTime (Opcional), Tipo: int

Especifique el período de retención en días. Los valores válidos son 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827 y 3653. El periodo de retención predeterminado es de 365 días.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

datasync-location-object-storage-usando-https

Comprueba si los servidores de almacenamiento de objetos de AWS DataSync ubicación utilizan el protocolo HTTPS para comunicarse. La regla NO ES COMPATIBLE si está configurada. ServerProtocol no es «HTTPS».

Identificador: DATASYNC_LOCATION_OBJECT_STORAGE_USING_HTTPS

Tipos de recursos: AWS::DataSync::LocationObjectStorage

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

datasync-task-data-verification-habilitado

Comprueba si AWS DataSync las tareas tienen habilitada la verificación de datos para realizar una verificación adicional al final de la transferencia. La regla no cumple con los requisitos de Configuration.options. VerifyMode es «NINGUNO».

Identificador: DATASYNC_TASK_DATA_VERIFICATION_ENABLED

Tipos de recursos: AWS::DataSync::Task

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

datasync-task-logging-enabled

Comprueba si una AWS DataSync tarea tiene activado el CloudWatch registro de Amazon. La regla es NON_COMPLIANT si una AWS DataSync tarea no tiene habilitado el CloudWatch registro de Amazon o si el nivel de registro no es equivalente al nivel de registro que especifiques.

Identificador: DATASYNC_TASK_LOGGING_ENABLED

Tipos de recursos: AWS::DataSync::Task

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

logLevel (opcional), Tipo: cadena

> Valor de cadena para el nivel de registro. Los valores válidos incluyen “BASIC” y “TRANSFER”. Si no se especifica nada, el valor predeterminado es “BASIC”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

datasync-task-tagged

Comprueba si AWS DataSync las tareas tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: DATASYNC_TASK_TAGGED

Tipos de recursos: AWS::DataSync::Task

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dax-encryption-enabled

Comprueba si los clústeres del Acelerador de Amazon DynamoDB (DAX) están cifrados. La regla es NON_COMPLIANT si el clúster de DAX no está cifrado.

Identificador: DAX_ENCRYPTION_ENABLED

Tipos de recursos: AWS::DAX::Cluster

Tipo de disparador: periódico

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), China (Pekín), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney), Europa (España) y China (Ningxia).

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dax-tls-endpoint-encryption

Comprueba si el clúster de Amazon DynamoDB Accelerator (DAX) está configurado en TLS. ClusterEndpointEncryptionType La regla es NON_COMPLIANT si hay un clúster de DAX que no está cifrado con seguridad de la capa de transporte (TLS).

Identificador: DAX_TLS_ENDPOINT_ENCRYPTION

Tipos de recursos: AWS::DAX::Cluster

Tipo de disparador: periódico

Región de AWS: solo está disponible en las regiones de Asia-Pacífico (Bombay), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

db-instance-backup-enabled

Comprueba si se han habilitado las copias de seguridad en las instancias de base de datos de RDS. Opcionalmente, la regla comprueba el periodo de retención de copia de seguridad y el periodo de tiempo de la copia de seguridad.

Identificador: DB_INSTANCE_BACKUP_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

backupRetentionMinimum (Opcional), Tipo: int

Periodo de retención mínimo de las copias de seguridad.

backupRetentionPeriod (Opcional), Tipo: int

El periodo de retención de las copias de seguridad.

checkReadReplicas (Opcional), Tipo: booleano

Comprueba si las instancias de base de datos de RDS tienen habilitadas las copias de seguridad para las réplicas de lectura.

preferredBackupWindow (Opcional), Tipo: cadena

El periodo de tiempo en el que se crean las copias de seguridad.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

desired-instance-tenancy

Comprueba si EC2 las instancias tienen un valor de «arrendamiento». También comprueba si IDs las AMI están especificadas para lanzarse desde esos hosts AMIs o si los hosts IDs se lanzan en esos hosts dedicados. La regla es COMPLIANT si la instancia coincide con un host y una AMI, si se especifica, en una lista.

Identificador: DESIRED_INSTANCE_TENANCY

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

tenencia, Tipo: cadena

Tenencia deseada de las instancias. Los valores válidos son DEDICATED, HOST y DEFAULT

imageId (opcional), Tipo: CSV

La regla evalúa las instancias lanzadas únicamente AMIs con lo especificado IDs. Separe varias AMI IDs con comas

hostId (opcional), Tipo: CSV

El IDs de los hosts EC2 dedicados en los que se van a lanzar las instancias. Separe varios hosts IDs con comas

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

desired-instance-type

Comprueba si EC2 las instancias son de un tipo de instancia específico. La regla es NON_COMPLIANT si no se especifica una EC2 instancia en la lista de parámetros. Para obtener una lista de los tipos de EC2 instancias compatibles, consulta los tipos de instancias en la Guía del EC2 usuario de instancias de Linux.

Identificador: DESIRED_INSTANCE_TYPE

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

instanceType, Tipo: CSV

Lista de tipos de EC2 instancias separados por comas (por ejemplo, «t2.small, m4.large, i2.xlarge»).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dms-auto-minor-version-verificación de actualizaciones

Comprueba si una instancia de replicación del AWS Database Migration Service (AWS DMS) tiene habilitadas las actualizaciones automáticas de versiones secundarias. La regla no cumple con los requisitos si una instancia de replicación del AWS DMS no está configurada con actualizaciones automáticas de versiones secundarias.

Identificador: DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

Tipos de recursos: AWS::DMS::ReplicationInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Zúrich) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dms-endpoint-ssl-configured

Comprueba si los puntos finales del AWS Database Migration Service (AWS DMS) están configurados con una conexión SSL. La regla NO ES COMPATIBLE si el AWS DMS no tiene configurada una conexión SSL.

Contexto: las conexiones SSL y TLS proporcionan una capa de seguridad al cifrar los datos que circulan entre el cliente y la instancia de base de datos. El uso de un certificado de servidor

proporciona una capa adicional de seguridad porque valida que se lleva a cabo una conexión a una instancia de base de datos de Amazon RDS. La validación ocurre al verificar que el certificado de servidor se instala automáticamente en todas las instancias de base de datos que usted aprovisione. Al activar la conexión SSL AWS DMS, se protege la confidencialidad de los datos durante la migración.

Para configurar la conexión SSL AWS DMS, consulte Uso para cifrar una conexión SSL/TLS a una instancia de base de datos o un clúster en la Guía del usuario de Amazon Relational Database Service.

Identificador: DMS_ENDPOINT_SSL_CONFIGURED

Tipos de recursos: AWS::DMS::Endpoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Zúrich) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dms-endpoint-tagged

Comprueba si los puntos finales AWS del DMS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: DMS_ENDPOINT_TAGGED

Tipos de recursos: AWS::DMS::Endpoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dms-mongo-db-authentication-habilitado

Comprueba si los puntos finales del AWS Database Migration Service (AWS DMS) para los almacenes de MongoDb datos están habilitados para la autenticación y el control de acceso basados en contraseñas. La regla es NON_COMPLIANT si la autenticación y el control de acceso basados en contraseñas no están habilitados.

Identificador: DMS_MONGO_DB_AUTHENTICATION_ENABLED

Tipos de recursos: AWS::DMS::Endpoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv),

Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dms-neptune-iam-authorization-habilitado

Comprueba si un punto final del AWS Database Migration Service (AWS DMS) para las bases de datos de Amazon Neptune está configurado con autorización de IAM. La regla no es compatible si un punto final del AWS DMS en el que Neptune es el objetivo se ha establecido en false. IamAuthEnabled

Identificador: DMS_NEPTUNE_IAM_AUTHORIZATION_ENABLED

Tipos de recursos: AWS::DMS::Endpoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá (Oeste) Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dms-redis-tls-enabled

Comprueba si los puntos finales del AWS Database Migration Service (AWS DMS) de los almacenes de datos de Redis están habilitados para el TLS/SSL cifrado de los datos comunicados con otros puntos finales. La regla no cumple con los requisitos si el cifrado no está activado. TLS/SSL

Identificador: DMS_REDIS_TLS_ENABLED

Tipos de recursos: AWS::DMS::Endpoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dms-replication-instance-multi-az-habilitado

Comprueba si las instancias de replicación del AWS Database Migration Service (DMS) están configuradas con varias zonas de disponibilidad. La regla es NON_COMPLIANT si una instancia de replicación de DMS no está configurada para usar varias zonas de disponibilidad.

Identificador: DMS_REPLICATION_INSTANCE_MULTI_AZ_ENABLED

Tipos de recursos: AWS::DMS::ReplicationInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico

(Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dms-replication-not-public

Comprueba si las instancias de replicación del AWS Database Migration Service (AWS DMS) son públicas. La regla no es compatible si el PubliclyAccessible campo está establecido en true.

Identificador: DMS_REPLICATION_NOT_PUBLIC

Tipos de recursos: AWS::DMS::ReplicationInstance

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dms-replication-task-sourcedb-registro

Comprueba si el registro está habilitado con un nivel de gravedad válido para las tareas de replicación del AWS DMS de una base de datos de origen. La regla es NON_COMPLIANT si el registro no está activado o si los registros de las tareas de replicación de DMS de una base de datos de origen tienen un nivel de gravedad que no es válido.

Identificador: DMS_REPLICATION_TASK_SOURCEDB_LOGGING

Tipos de recursos: AWS::DMS::ReplicationTask

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dms-replication-task-tagged

Comprueba si las tareas de replicación del AWS DMS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: DMS_REPLICATION_TASK_TAGGED

Tipos de recursos: AWS::DMS::ReplicationTask

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dms-replication-task-targetdb-registro

Comprueba si el registro está habilitado con un nivel de gravedad válido para los eventos de las tareas de replicación del AWS DMS de una base de datos de destino. La regla es NON_COMPLIANT si el registro no está activado o si los registros de las tareas de replicación de una base de datos de destino tienen un nivel de gravedad que no es válido.

Identificador: DMS_REPLICATION_TASK_TARGETDB_LOGGING

Tipos de recursos: AWS::DMS::ReplicationTask

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

docdb-cluster-audit-logging-habilitado

Comprueba si un clúster de instancias de Amazon DocumentDB (compatible con MongoDB) tiene habilitada la exportación de registros para los CloudWatch registros de auditoría. La regla es NON_COMPLIANT si un clúster de instancias de Amazon DocumentDB no CloudWatch tiene habilitada la exportación de registros para los registros de auditoría.

Identificador: DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Europa (Estocolmo), Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Centro), EE.UU. Oeste (Norte de California), Israel (Tel Aviv), Región Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

docdb-cluster-backup-retention-comprobar

Comprueba si el período de retención de un clúster de Amazon DocumentDB está establecido en un número específico de días. La regla es NON_COMPLIANT si el período de retención es inferior al valor especificado por el parámetro.

Identificador: DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Europa (Estocolmo), Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Centro), EE.UU. Oeste (Norte de California), Israel (Tel Aviv), Región Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Europa (Zúrich)

Parámetros:

minimumBackupRetentionPeriodo (opcional), Tipo: int

> Las copias de seguridad se deben conservar un mínimo de días. Los valores válidos son del 1 al 35; el valor predeterminado es 7. Esta regla no cumple con los requisitos si el valor es mayor que ". backupRetentionPeriod

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

docdb-cluster-deletion-protection-habilitado

Comprueba si un clúster de Amazon DocumentDB (compatible con MongoDB) tiene habilitada la protección contra eliminación. La regla es NON_COMPLIANT si un clúster de Amazon DocumentDB tiene el campo DeletionProtection establecido en false.

Identificador: DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Europa (Estocolmo), Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Centro), EE.UU. Oeste (Norte de California), Israel (Tel Aviv), Región Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

docdb-cluster-encrypted

Comprueba si el cifrado de almacenamiento está activado en los clústeres de Amazon DocumentDB (con compatibilidad con MongoDB). La regla es NON_COMPLIANT si el cifrado de almacenamiento no está habilitado.

Identificador: DOCDB_CLUSTER_ENCRYPTED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Europa (Estocolmo), Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Centro), EE.UU. Oeste (Norte de California), Israel (Tel Aviv), Región Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Europa (Zúrich)

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

> Una lista de claves de KMS separada por comas ARNs para compararla con el KmsKey ID del clúster cifrado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

docdb-cluster-encrypted-in-tránsito

Comprueba si las conexiones a los clústeres de Amazon DocumentDB están configuradas para utilizar cifrado en tránsito. La regla es NON_COMPLIANT si el grupo de parámetros no está “sincronizado” o si el parámetro TLS está establecido en “disabled” o en un valor en `excludeTlsParameters`.

Identificador: DOCDB_CLUSTER_ENCRYPTED_IN_TRANSIT

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto Europa (Estocolmo), Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Centro), EE.UU. Oeste (Norte de California), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región Europa (España), Europa (Zúrich)

Parámetros:

excludeTlsParameters (Opcional), Tipo: CSV

> Lista separada por comas de parámetros del clúster de TLS para que la regla NO los compruebe. Valor predeterminado: “disabled”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

docdb-cluster-snapshot-public-prohibido

Comprueba si las instantáneas del clúster manual de Amazon DocumentDB son públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

Identificador: DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

Tipos de recursos: AWS::RDS::DBClusterSnapshot

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Medio Oriente (EAU), Europa (Fráncfort), América del Sur (São Paulo), Asia-Pacífico (Hong Kong), Asia-Pacífico (Hyderabad), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Europa (Milán), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dynamodb-autoscaling-enabled

Comprueba si las tablas de Amazon DynamoDB o los índices secundarios globales pueden read/write procesar la capacidad mediante el modo bajo demanda o el modo aprovisionado con el escalado automático activado. La regla es NON_COMPLIANT si se utiliza alguno de los modos sin activar el escalado automático.

Identificador: DYNAMODB_AUTOSCALING_ENABLED

Tipos de recursos: AWS::DynamoDB::Table

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

minProvisionedReadCapacidad (opcional), Tipo: int

Cantidad mínima de unidades con capacidad de lectura que debería aprovisionarse en el grupo de escalado automático.

maxProvisionedReadCapacidad (opcional), Tipo: int

Cantidad máxima de unidades con capacidad de lectura que deberían aprovisionarse en el grupo de escalado automático.

targetReadUtilization (Opcional), Tipo: double

El porcentaje de objetivo de utilización de capacidad de lectura. El objetivo de utilización se expresa como la proporción de unidades de capacidad consumidas respecto de la capacidad aprovisionada.

minProvisionedWriteCapacidad (opcional), Tipo: int

Cantidad mínima de unidades con capacidad de escritura que debería aprovisionarse en el grupo de escalado automático.

maxProvisionedWriteCapacidad (opcional), Tipo: int

Cantidad máxima de unidades con capacidad de escritura que debería aprovisionarse en el grupo de escalado automático.

targetWriteUtilization (Opcional), Tipo: double

El porcentaje de objetivo de utilización de capacidad de escritura. El objetivo de utilización se expresa como la proporción de unidades de capacidad consumidas respecto de la capacidad aprovisionada.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dynamodb-in-backup-plan

Comprueba si la tabla Amazon DynamoDB está presente en AWS los planes de Backup. La regla no es conforme si las tablas de Amazon DynamoDB no están presentes en ningún plan de Backup. AWS

Identificador: DYNAMODB_IN_BACKUP_PLAN

Tipos de recursos: AWS::DynamoDB::Table

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dynamodb-last-backup-recovery-punto creado

Comprueba si se ha creado un punto de recuperación para las tablas de Amazon DynamoDB dentro del periodo especificado. La regla es NON_COMPLIANT si la tabla de DynamoDB no tiene ningún punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::DynamoDB::Table

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de las tablas de DynamoDB para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

Nombre de la tabla de DynamoDB que debe comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dynamodb-meets-restore-time-objetivo

Compruebe si el tiempo de restauración de las tablas de Amazon DynamoDB cumple con la duración especificada. La regla es NON_COMPLIANT si LatestRestoreExecutionTimeMinutes una tabla de DynamoDB es superior a minutos. maxRestoreTime

Identificador: DYNAMODB_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::DynamoDB::Table

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

maxRestoreTime, Tipo: int

Valor numérico del tiempo de ejecución de restauración máximo permitido.

resourceTags (opcional), Tipo: cadena

Etiquetas de las tablas de DynamoDB para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

Nombre de la tabla de DynamoDB que debe comprobar la regla.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dynamodb-pitr-enabled

Comprueba si point-in-time la recuperación (PITR) está habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.

Identificador: DYNAMODB_PITR_ENABLED

Tipos de recursos: AWS::DynamoDB::Table

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dynamodb-resources-protected-by-plan de respaldo

Comprueba si las tablas de Amazon DynamoDB están protegidas por un plan de copia de seguridad. La regla es NON_COMPLIANT si la tabla de DynamoDB no está cubierta por un plan de copia de seguridad.

Identificador: DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::DynamoDB::Table

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas para las tablas de DynamoDB para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

Nombre de la tabla de DynamoDB que debe comprobar la regla.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

dynamodb-table-deletion-protection-habilitado

Comprueba si una tabla de Amazon DynamoDB tiene habilitada la protección contra eliminaciones. La regla es NON_COMPLIANT si la tabla tiene la protección de eliminación desactivada.

Identificador: DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::DynamoDB::Table

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dynamodb-table-encrypted-kms

Comprueba si la tabla de Amazon DynamoDB está cifrada AWS con el Servicio de administración de claves (KMS). La regla no es compatible si la tabla de Amazon DynamoDB no está cifrada con KMS. AWS La regla tampoco cumple con los requisitos si la clave de AWS KMS cifrada no está presente en el parámetro de entrada. `kmsKeyArns`

Identificador: DYNAMODB_TABLE_ENCRYPTED_KMS

Tipos de recursos: AWS::DynamoDB::Table

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

> Lista separada por comas de claves de AWS KMS ARNs permitidas para cifrar tablas de Amazon DynamoDB

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dynamodb-table-encryption-enabled

Comprueba si las tablas de Amazon DynamoDB están cifradas y verifica su estado. La regla es COMPLIANT si el estado indica que se han habilitado o se están habilitando.

Identificador: DYNAMODB_TABLE_ENCRYPTION_ENABLED

Tipos de recursos: AWS::DynamoDB::Table

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

dynamodb-throughput-limit-check

Comprueba si el rendimiento aprovisionado de DynamoDB se acerca al límite máximo de su cuenta. De forma predeterminada, la regla comprueba si el rendimiento aprovisionado supera el umbral del 80 % de los límites de su cuenta.

Identificador: DYNAMODB_THROUGHPUT_LIMIT_CHECK

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

RCUThresholdPorcentaje de cuenta (opcional), Tipo: int, Valor predeterminado: 80

Porcentaje de unidades de capacidad de lectura aprovisionadas para su cuenta. Cuando se alcanza este valor, la regla se marca como no conforme.

WCUThresholdporcentaje de cuenta (opcional), Tipo: int, Valor predeterminado: 80

Porcentaje de unidades de capacidad de escritura aprovisionadas para su cuenta. Cuando se alcanza este valor, la regla se marca como no conforme.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ebs-in-backup-plan

Compruebe si los volúmenes de Amazon Elastic Block Store (Amazon EBS) se añaden a los planes de backup de Backup. AWS La regla es NON_COMPLIANT si los volúmenes de Amazon EBS no están incluidos en los planes de copia de seguridad.

Identificador: EBS_IN_BACKUP_PLAN

Tipos de recursos: AWS::EC2::Volume

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ebs-last-backup-recovery-punto creado

Comprueba si se ha creado un punto de recuperación para Amazon Elastic Block Store (Amazon EBS). La regla es NON_COMPLIANT si el volumen de Amazon EBS no tiene un punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::EC2::Volume

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Amazon EBS para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID del volumen de Amazon EBS que debe comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ebs-meets-restore-time-objetivo

Comprueba si el tiempo de restauración de los volúmenes de Amazon Elastic Block Store (Amazon EBS) cumple con la duración especificada. La regla es NON_COMPLIANT si el volumen LatestRestoreExecutionTimeMinutes de Amazon EBS es superior a minutos. maxRestoreTime

Identificador: EBS_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::EC2::Volume

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

maxRestoreTime, Tipo: int

Valor numérico del tiempo de ejecución de restauración máximo permitido.

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Amazon EBS para que la regla las compruebe, en formato JSON .

resourceId (opcional), Tipo: cadena

ID del volumen de Amazon EBS que debe comprobar la regla.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ebs-optimized-instance

Comprueba si la optimización de Amazon EBS está habilitada para las instancias de Amazon Elastic Compute Cloud (Amazon EC2) que pueden optimizarse para Amazon EBS. La regla es NON_COMPLIANT si la optimización de EBS no está habilitada para una EC2 instancia de Amazon que pueda optimizarse para EBS.

> **Note**
>
> EC2 Las instancias que están optimizadas para EBS de forma predeterminada siempre hacen que se devuelvan las evaluaciones de las reglas. `COMPLIANT`

Identificador: EBS_OPTIMIZED_INSTANCE

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ebs-resources-in-logically-air-gapped-vault

Comprueba si los volúmenes de Amazon Elastic Block Store (Amazon EBS) están dentro de un almacén aislado lógicamente. La regla es NON_COMPLIANT si hay un volumen de Amazon EBS que no está en un almacén aislado lógicamente dentro del período de tiempo especificado.

Identificador: EBS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Tipos de recursos: AWS::EC2::Volume

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Amazon EBS para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID del volumen de Amazon EBS que debe comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 2184 horas y 91 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ebs-resources-protected-by-plan de respaldo

Comprueba si los volúmenes de Amazon Elastic Block Store (Amazon EBS) están protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el volumen de Amazon EBS no está cubierto por un plan de copia de seguridad.

Identificador: EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::EC2::Volume

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Amazon EBS para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID del volumen de Amazon EBS que debe comprobar la regla.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ebs-snapshot-block-public-acceso

Comprueba si el bloqueo del acceso público está activado para las instantáneas de Amazon EBS en una AWS región. La regla no cumple con los requisitos si el bloqueo del acceso público no está habilitado para compartir en público todas las instantáneas de EBS de una región. AWS

Identificador: EBS_SNAPSHOT_BLOCK_PUBLIC_ACCESS

Tipos de recursos: AWS::EC2::SnapshotBlockPublicAccess

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ebs-snapshot-public-restorable-comprobar

Comprueba si las instantáneas de Amazon Elastic Block Store (Amazon EBS) no se pueden restaurar públicamente. La regla es NON_COMPLIANT si una o más instantáneas con el RestorableByUserIds campo están configuradas como todas, es decir, las instantáneas de Amazon EBS son públicas.

Identificador: EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles excepto la región de Europa (España)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 capacity-reservation-tagged

Comprueba si las reservas EC2 de capacidad de Amazon tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EC2 _CAPACITY_RESERVATION_TAGGED

Tipos de recursos: AWS::EC2::CapacityReservation

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 carrier-gateway-tagged

Comprueba si las pasarelas de EC2 transporte de Amazon tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _CARRIER_GATEWAY_TAGGED EC2

Tipos de recursos: AWS::EC2::CarrierGateway

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec2- activado client-vpn-connection-log

Comprueba si el punto final AWS Client VPN tiene activado el registro de conexiones de clientes. La regla no cumple con los requisitos si es «Configuración». ConnectionLogOptions.Enabled' se establece en falso.

Identificador: _CLIENT_VPN_CONNECTION_LOG_ENABLED EC2

Tipos de recursos: AWS::EC2::ClientVpnEndpoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 client-vpn-endpoint-tagged

Comprueba si los puntos de conexión VPN de los EC2 clientes de Amazon tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _CLIENT_VPN_ENDPOINT_TAGGED EC2

Tipos de recursos: AWS::EC2::ClientVpnEndpoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Centro), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Región (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- -todos client-vpn-not-authorize

Comprueba si las reglas de autorización de AWS Client VPN autorizan el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.

Identificador: _CLIENT_VPN_NOT_AUTHORIZE_ALL EC2

Tipos de recursos: AWS::EC2::ClientVpnEndpoint

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 dhcp-options-tagged

Comprueba si las opciones de Amazon EC2 DHCP tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _DHCP_OPTIONS_TAGGED EC2

Tipos de recursos: AWS::EC2::DHCPOptions

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 ebs-encryption-by-default

Comprueba si el cifrado de Amazon Elastic Block Store (EBS) está activado de forma predeterminada. La regla es NON_COMPLIANT si el cifrado no se ha habilitado.

Identificador: _EBS_ENCRYPTION_BY_DEFAULT EC2

Tipo de disparador: periódico

Región de AWS: Todas las regiones compatibles AWS

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- activado enis-source-destination-check

Comprueba source/destination si las opciones gestionadas por los usuarios tienen habilitada la opción de verificación. EC2 ENIs La regla no cumple con las normas si source/destination están desactivadas las ENIs opciones «lambda», «aws_codestar_connections_managed», «branch», «efa», «interface» y «quicksight».

EC2Identificador: _ENIS_SOURCE_DESTINATION_CHECK_ENABLED

Tipos de recursos: AWS::EC2::NetworkInterface

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec2-fleet-tagged

Comprueba si EC2 las flotas de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _FLEET_TAGGED EC2

Tipos de recursos: 2Fleet AWS::EC2::EC

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec2-imdsv2-check

Comprueba si la versión de metadatos de la instancia de Amazon Elastic Compute Cloud (Amazon EC2) está configurada con la versión 2 (IMDSv2) del servicio de metadatos de la instancia. La regla no cumple con los requisitos si HttpTokens se establece en opcional.

Identificador: _ _CHECK EC2 IMDSV2

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 instance-detailed-monitoring-enabled

Comprueba si la supervisión detallada está habilitada para EC2 las instancias. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.

Identificador: EC2 _INSTANCE_DETAILED_MONITORING_ENABLED

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 -ami instance-launched-with-allowed

Comprueba si las EC2 instancias en ejecución o detenidas se lanzaron con Amazon Machine Images (AMIs) que cumplen AMIs los criterios permitidos. La regla no es compatible si una AMI no cumple con los AMIs criterios permitidos y la AMIs configuración permitida no está deshabilitada.

Identificador: _INSTANCE_LAUNCHED_WITH_ALLOWED_AMI EC2

Tipos de recursos: AWS::EC2::Instance

Tipo de desencadenador: cambios de configuración y periódicos

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

InstanceStateNameList (Opcional), Tipo: CSV

> Lista de estados de EC2 instancia de Amazon separados por comas para que la regla los compruebe. Los valores válidos son “running” y “stopped”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- -administrador instance-managed-by-systems

> **Important**
>
> Para esta regla, el identificador de la regla (EC2_INSTANCE_MANAGED_BY_SSM) y el nombre de la regla (ec2- -manager) son diferentes. instance-managed-by-systems

Comprueba si tus EC2 instancias de Amazon están gestionadas por AWS Systems Manager un agente (SSM Agent). La regla no cumple con los requisitos si una EC2 instancia está en ejecución y el agente SSM está detenido, o si una EC2 instancia se está ejecutando y el agente SSM está cerrado.

> **Note**
>
> La regla no devolverá NON_COMPLIANT si una EC2 instancia está detenida y el agente SSM está en ejecución.

Identificador: _INSTANCE_MANAGED_BY_SSM EC2

Tipos de recursos:, AWS::EC2::Instance AWS::SSM::ManagedInstanceInventory

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 instance-multiple-eni-check

Comprueba si Amazon Elastic Compute Cloud (Amazon EC2) utiliza varias interfaces de red elásticas (ENIs) o adaptadores Elastic Fabric (EFAs). La regla es NON_COMPLIANT: una EC2 instancia de Amazon utiliza varias interfaces de red.

Identificador: _INSTANCE_MULTIPLE_ENI_CHECK EC2

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

NetworkInterfaceIds (Opcional), Tipo: CSV

Lista de instancias de red separadas por comas IDs

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con AWS Config reglas. Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 instance-no-public-ip

Comprueba si las instancias de Amazon Elastic Compute Cloud (Amazon EC2) tienen una asociación de IP pública. La regla es NON_COMPLIANT si el campo publicIP está presente en el elemento de configuración de la EC2 instancia de Amazon. Esta regla se aplica únicamente a. IPv4

Contexto: las direcciones IP públicas pueden hacer que las EC2 instancias sean accesibles directamente desde Internet, lo que puede no ser siempre deseable desde el punto de vista de la seguridad o el cumplimiento:

- Seguridad: en muchos casos, es posible que no desees que tus EC2 instancias tengan direcciones IP públicas, a menos que sea necesario que sean de acceso público. Tener una dirección IP pública puede exponer la EC2 instancia a posibles riesgos de seguridad, como ataques o accesos no autorizados.

- Cumplimiento: varios estándares de cumplimiento, como PCI, DSS o HIPAA, tienen requisitos específicos en relación con la segmentación de la red y los controles de acceso. Garantizar que EC2 las instancias no tengan direcciones IP públicas innecesarias puede ayudar a garantizar el cumplimiento de estos requisitos.
- Administración de costos: las direcciones IP públicas pueden generar costos adicionales, especialmente si hay EC2 instancias asociadas continuamente a ellas. Al identificar EC2 las instancias públicas IPs que no las necesitan, puede reducir los costos.

Identificador: EC2 _INSTANCE_NO_PUBLIC_IP

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 instance-profile-attached

Comprueba si una EC2 instancia tiene un perfil de AWS Identity and Access Management (IAM) adjunto. La regla no cumple con las normas si no hay ningún perfil de IAM adjunto a la instancia. EC2

Identificador: _INSTANCE_PROFILE_ATTACHED EC2

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EEUU-Este), AWS GovCloud (EEUU-Oeste) y China (Ningxia)

Parámetros:

IamInstanceProfileArnList (Opcional), Tipo: CSV

Lista separada por comas de los nombres de recursos de Amazon (ARNs) del perfil de IAM que se pueden adjuntar a las instancias de Amazon. EC2

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec2- -creado last-backup-recovery-point

Comprueba si se creó un punto de recuperación para las instancias de Amazon Elastic Compute Cloud (Amazon EC2). La regla es NON_COMPLIANT si la EC2 instancia de Amazon no tiene un punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: _LAST_BACKUP_RECOVERY_POINT_CREATED EC2

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de las EC2 instancias de Amazon para que la regla las compruebe, en formato JSON`{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID de la EC2 instancia de Amazon para comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec2- encriptado launch-templates-ebs-volume

Comprueba si las plantillas de EC2 lanzamiento de Amazon tienen el cifrado activado para todos los volúmenes de EBS adjuntos. La regla es NON_COMPLIANT si el cifrado se establece en False para cualquier volumen de EBS configurado en la plantilla de lanzamiento.

EC2Identificador: _LAUNCH_TEMPLATES_EBS_VOLUME_ENCRYPTED

Tipos de recursos: AWS::EC2::LaunchTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec2- 2-check launch-template-imdsv

Comprueba si la versión predeterminada establecida actualmente de una plantilla de EC2 lanzamiento de Amazon requiere que las nuevas instancias lanzadas utilicen la versión 2 del

Amazon EC2 Instance Metadata Service (IMDSv2). La regla no cumple con los requisitos si la «versión de metadatos» no se especifica como V2 (). IMDSv2

Identificador: _LAUNCH_TEMPLATE_ _CHECK EC2 IMDSV2

Tipos de recursos: AWS::EC2::LaunchTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- -deshabilitado launch-template-public-ip

Comprueba si las plantillas de EC2 lanzamiento de Amazon están configuradas para asignar direcciones IP públicas a las interfaces de red. La regla no es conforme si la versión predeterminada de una plantilla de EC2 lanzamiento tiene al menos una interfaz de red con el valor «AssociatePublicIpAddressverdadero».

EC2Identificador: _LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

Tipos de recursos: AWS::EC2::LaunchTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv),

Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich) AWS GovCloud

Parámetros:

exemptedLaunchTemplates (Opcional), Tipo: CSV

Lista separada por comas de plantillas de EC2 lanzamiento exentas IDs que pueden tener interfaces de red con el AssociatePublicIpAddress valor establecido en «true».

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 launch-template-tagged

Comprueba si las plantillas de EC2 lanzamiento de Amazon tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EC2 _LAUNCH_TEMPLATE_TAGGED

Tipos de recursos: AWS::EC2::LaunchTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 managedinstance-applications-blacklisted

Comprueba que ninguna de las aplicaciones especificadas esté instalada en la instancia. Si lo desea, especifique la versión. Las versiones más recientes no se excluirán de la lista. Opcionalmente, especifique la plataforma para aplicar la regla únicamente en las instancias que se ejecuten en dicha plataforma.

Identificador: _MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED EC2

Tipos de recursos: AWS::SSM::ManagedInstanceInventory

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de Asia Pacífico (Taipéi)

Parámetros:

applicationNames, Tipo: CSV

Lista separada por comas de nombres de aplicaciones. Opcionalmente, especifique las versiones con “:” (por ejemplo, Chrome:0.5.3, FireFox).

> **Note**
>
> Los nombres de aplicación deben ser coincidencias exactas. Por ejemplo, use **`firefox`** en Linux o **`firefox-compat`** en Amazon Linux. Además, actualmente no AWS Config admite caracteres comodín para el parámetro ApplicationNames (por ejemplo**`firefox*`**,).

platformType (opcional), Tipo: cadena

Tipo de plataforma (por ejemplo, Linux o Windows).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 managedinstance-applications-required

Comprueba que todas las aplicaciones especificadas estén instaladas en la instancia. Opcionalmente, especifique la versión mínima aceptable. También puede especificar la plataforma para aplicar la regla únicamente en las instancias que se ejecuten en dicha plataforma.

> **Note**
>
> Asegúrese de que el agente SSM se esté ejecutando en la EC2 instancia y de que se cree una asociación para recopilar el inventario del software de la aplicación. La regla devuelve `NOT_APPLICABLE` si el agente de SSM no está instalado o si aún no se ha creado o no se está ejecutando una asociación.

Identificador: _MANAGEDINSTANCE_APPLICATIONS_REQUIRED EC2

Tipos de recursos: AWS::SSM::ManagedInstanceInventory

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de Asia Pacífico (Taipéi)

Parámetros:

applicationNames, Tipo: CSV

Lista separada por comas de nombres de aplicaciones. Opcionalmente, especifique las versiones con “:” (por ejemplo, Chrome:0.5.3, FireFox).

> **Note**
>
> Los nombres de aplicación deben ser coincidencias exactas. Por ejemplo, use **`firefox`** en Linux o **`firefox-compat`** en Amazon Linux. Además, actualmente no AWS Config admite caracteres comodín para el parámetro ApplicationNames (por ejemplo**`firefox*`**,).

platformType (opcional), Tipo: cadena

Tipo de plataforma (por ejemplo, Linux o Windows).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec2- -comprobar managedinstance-association-compliance-status

Comprueba si el estado de conformidad de la asociación de AWS Systems Manager es COMPLIANT o NON_COMPLIANT tras la ejecución de la asociación en la instancia. La regla se cumple si el estado del campo es COMPLIANT. Para obtener más información sobre las asociaciones, consulte ¿Qué es una asociación?.

Identificador: _MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK EC2

Tipos de recursos: AWS::SSM::AssociationCompliance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Osaka), (EE. UU. Este) AWS GovCloud AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 managedinstance-inventory-blacklisted

Comprueba si las instancias gestionadas por Amazon EC2 Systems Manager están configuradas para recopilar tipos de inventario incluidos en la lista negra.

Identificador: _MANAGEDINSTANCE_INVENTORY_BLACKLISTED EC2

Tipos de recursos: AWS::SSM::ManagedInstanceInventory

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de Asia Pacífico (Taipéi)

Parámetros:

inventoryNames, Tipo: CSV

Lista de tipos de inventario de Systems Manager separados por comas (por ejemplo, ':Network AWS,: AWS'). WindowsUpdate

platformType (opcional), Tipo: cadena

Tipo de plataforma (por ejemplo, Linux).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- -comprobar managedinstance-patch-compliance-status

Comprueba si el estado de conformidad del parche de AWS Systems Manager es CONFORME o NO CONFORME tras la instalación del parche en la instancia. La regla se cumple si el estado del campo es COMPLIANT.

Identificador: _MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK EC2

Tipos de recursos: AWS::SSM::PatchCompliance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Osaka), Europa (Milán) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 managedinstance-platform-check

Comprueba si las instancias EC2 gestionadas tienen las configuraciones deseadas.

Identificador: EC2 _MANAGEDINSTANCE_PLATFORM_CHECK

Tipos de recursos: AWS::SSM::ManagedInstanceInventory

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de Asia Pacífico (Taipéi)

Parámetros:

platformType, Tipo: cadena

Tipo de plataforma (por ejemplo, Linux).

platformVersion (opcional), Tipo: cadena

Versión de la plataforma (por ejemplo, 2016.09).

agentVersion (opcional), Tipo: cadena

Versión del agente (por ejemplo, 2.0.433.0).

platformName (opcional), Tipo: cadena

Versión de la plataforma (por ejemplo, 2016.09).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 meets-restore-time-target

Comprueba si el tiempo de restauración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) cumple con la duración especificada. La regla es NON_COMPLIANT si LatestRestoreExecutionTimeMinutes una EC2 instancia de Amazon es superior maxRestoreTime a minutos.

Identificador: _MEETS_RESTORE_TIME_TARGET EC2

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

maxRestoreTime, Tipo: int

Valor numérico del tiempo de ejecución de restauración máximo permitido.

resourceTags (opcional), Tipo: cadena

Etiquetas de las EC2 instancias de Amazon para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID de la EC2 instancia de Amazon que debe comprobar la regla.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- network-insights-access-scope -análisis-etiquetado

Comprueba si los análisis del alcance de acceso de Amazon EC2 Network Insights tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o

si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EC2 _NETWORK_INSIGHTS_ACCESS_SCOPE_ANALYSIS_TAGGED

Tipos de recursos: AWS::EC2::NetworkInsightsAccessScopeAnalysis

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- -etiquetado network-insights-access-scope

Comprueba si los ámbitos de acceso a Amazon EC2 Network Insights tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _NETWORK_INSIGHTS_ACCESS_SCOPE_TAGGED EC2

Tipos de recursos: AWS::EC2::NetworkInsightsAccessScope

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 network-insights-analysis-tagged

Comprueba si los análisis EC2 de Amazon Network Insights tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EC2 _NETWORK_INSIGHTS_ANALYSIS_TAGGED

Tipos de recursos: AWS::EC2::NetworkInsightsAnalysis

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este)

AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 network-insights-path-tagged

Comprueba si las rutas EC2 de Amazon Network Insights tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EC2 _NETWORK_INSIGHTS_PATH_TAGGED

Tipos de recursos: AWS::EC2::NetworkInsightsPath

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 no-amazon-key-pair

Comprueba si las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución se lanzan con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una EC2 instancia en ejecución con un key pair.

Identificador: _NO_AMAZON_KEY_PAIR EC2

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 paravirtual-instance-check

Comprueba si el tipo de virtualización de una instancia es paravirtual. EC2 Esta regla no cumple con los requisitos para una EC2 instancia si 'VirtualizationType' está configurado como 'paravirtual'.

Identificador EC2: _PARAVIRTUAL_INSTANCE_CHECK

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: solo disponible en China (Pekín), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 prefix-list-tagged

Comprueba si las listas de EC2 prefijos gestionadas por Amazon tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _PREFIX_LIST_TAGGED EC2

Tipos de recursos: AWS::EC2::PrefixList

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- -bóveda con huecos resources-in-logically-air

Comprueba si las instancias de Amazon Elastic Compute Cloud (Amazon EC2) se encuentran en una bóveda aislada de forma lógica. La regla es NON_COMPLIANT si una EC2 instancia de Amazon no se encuentra en un almacén con huecos lógicos dentro del período de tiempo especificado.

Identificador EC2: _RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de las EC2 instancias de Amazon para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID de la EC2 instancia de Amazon que debe comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 2184 horas y 91 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

plan ec2 resources-protected-by-backup

Comprueba si las instancias de Amazon Elastic Compute Cloud (Amazon EC2) están protegidas por un plan de respaldo. La regla es NON_COMPLIANT si la EC2 instancia de Amazon no está cubierta por un plan de respaldo.

> **Note**
>
> Esta regla solo se aplica a las EC2 instancias de Amazon en ejecución y no a las instancias que están apagadas.

Identificador: EC2 _RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas para EC2 las instancias de Amazon para que la regla las compruebe, en formato JSON`{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID de la EC2 instancia de Amazon para comprobar la regla.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 security-group-attached-to -es

Comprueba que los grupos de seguridad no predeterminados estén conectados a las instancias de Amazon Elastic Compute Cloud (EC2) o a una interfaz de red elástica (ENIs). La regla devuelve NON_COMPLIANT si el grupo de seguridad no está asociado a una EC2 instancia o a un ENI.

Identificador: _SECURITY_GROUP_ATTACHED_TO_ENI EC2

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Emiratos Árabes Unidos) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- -eni-periódico security-group-attached-to

Comprueba si los grupos de seguridad no predeterminados están conectados a las interfaces de red de Elastic ()ENIs. La regla es NON_COMPLIANT si el grupo de seguridad no está asociado a una ENI. Los grupos de seguridad que no son propiedad de la cuenta que realiza la llamada se evalúan como NOT_APPLICABLE.

> **Note**
>
> Esta regla informa sobre el tipo de recurso `AWS::EC2::SecurityGroup`. Sin embargo, para que la regla se ejecute de forma eficaz, debe habilitar el registro del tipo de recurso `AWS::EC2::NetworkInterface`.

Identificador: _SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC EC2

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- - spot-fleet-request-ct encryption-at-rest

Comprueba si los parámetros de lanzamiento de la solicitud de Amazon EC2 Spot Fleet están cifrados en True para los volúmenes de EBS adjuntos. La regla es NON_COMPLIANT si algún volumen de EBS tiene el cifrado establecido en Falso. La regla no evalúa las solicitudes de flota de spot mediante plantillas de lanzamiento.

Identificador: _SPOT_FLEET_REQUEST_CT_ENCRYPTION_AT_REST EC2

Tipos de recursos: AWS::EC2::SpotFleet

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en Europa (Irlanda), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Oeste de EE. UU. (Oregón), China (Ningxia) y Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2-stopped-instance

Comprueba si hay instancias de Amazon Elastic Compute Cloud (Amazon EC2) detenidas durante más días del permitido. La regla es NON_COMPLIANT si el estado de una EC2 instancia de Amazon ha estado detenida durante más tiempo del permitido o si no se puede determinar el período de tiempo.

Identificador: _STOPPED_INSTANCE EC2

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

AllowedDays (Opcional), Tipo: int, Valor predeterminado: 30

El número de días que se puede detener una EC2 instancia de Amazon antes de que la regla sea NON_COMPLIANT. El número predeterminado de días es 30.

> **Note**
>
> El número de días seleccionado debe ser inferior al período de retención configurado, ya que esta regla se basa en los datos históricos recopilados. Para obtener más información sobre la retención de datos históricos, consulta Eliminar AWS Config datos.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 token-hop-limit-check

Comprueba si los metadatos de una instancia de Amazon Elastic Compute Cloud (EC2) tienen un límite de salto de token especificado inferior al límite deseado. La regla es NON_COMPLIANT para una instancia si tiene un valor de límite de saltos superior al límite previsto.

Identificador: EC2 _TOKEN_HOP_LIMIT_CHECK

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

tokenHopLimit (Opcional), Tipo: int

Límite de salto de tokens deseado. Los valores válidos están entre 1 y 64, ambos inclusive. El valor predeterminado es 1 si no se especifica ningún parámetro.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 traffic-mirror-filter-description

Comprueba si los filtros espejo de EC2 tráfico de Amazon tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe.

Identificador: EC2 _TRAFFIC_MIRROR_FILTER_DESCRIPTION

Tipos de recursos: AWS::EC2::TrafficMirrorFilter

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 traffic-mirror-filter-tagged

Comprueba si los filtros espejo de EC2 tráfico de Amazon tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o

si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EC2 _TRAFFIC_MIRROR_FILTER_TAGGED

Tipos de recursos: AWS::EC2::TrafficMirrorFilter

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 traffic-mirror-session-description

Comprueba si las sesiones espejo de EC2 tráfico de Amazon tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe.

Identificador: EC2 _TRAFFIC_MIRROR_SESSION_DESCRIPTION

Tipos de recursos: AWS::EC2::TrafficMirrorSession

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes

Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Europa (Milán), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary)), Región de Europa (España), China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 traffic-mirror-session-tagged

Comprueba si las sesiones espejo de EC2 tráfico de Amazon tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EC2 _TRAFFIC_MIRROR_SESSION_TAGGED

Tipos de recursos: AWS::EC2::TrafficMirrorSession

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Europa (Milán), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary)), Región de Europa (España), China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 traffic-mirror-target-description

Comprueba si los objetivos espejo de EC2 tráfico de Amazon tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe.

Identificador: EC2 _TRAFFIC_MIRROR_TARGET_DESCRIPTION

Tipos de recursos: AWS::EC2::TrafficMirrorTarget

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Centro), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), Región de China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 traffic-mirror-target-tagged

Comprueba si los objetivos espejo de EC2 tráfico de Amazon tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EC2 _TRAFFIC_MIRROR_TARGET_TAGGED

Tipos de recursos: AWS::EC2::TrafficMirrorTarget

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), Región de China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec2- -attach-desactivado transit-gateway-auto-vpc

Comprueba si las pasarelas de tránsito de Amazon Elastic Compute Cloud (Amazon EC2) tienen 'AutoAcceptSharedAttachments' habilitado. La regla no es conforme para una Transit Gateway si 'AutoAcceptSharedAttachments' está configurada como 'activa'.

Identificador EC2: _TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

Tipos de recursos: AWS::EC2::TransitGateway

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec2- -etiquetado transit-gateway-multicast-domain

Comprueba si los dominios de multidifusión de Amazon EC2 Transit Gateway tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _TRANSIT_GATEWAY_MULTICAST_DOMAIN_TAGGED EC2

Tipos de recursos: AWS::EC2::TransitGatewayMulticastDomain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ec-2 volume-inuse-check

Comprueba si los volúmenes de EBS están adjuntos a EC2 las instancias. Opcionalmente, comprueba si los volúmenes de EBS se marcan para eliminarse cuando se termina una instancia.

La regla cumple con los requisitos si un volumen de EBS está adjunto a instancias en ejecución o detenidas EC2 .

La regla no cumple con los requisitos si un volumen de EBS no está adjunto a ninguna EC2 instancia o si está adjunto a una instancia finalizada. EC2

Identificador: _VOLUME_INUSE_CHECK EC2

Tipos de recursos: AWS::EC2::Volume

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EEUU-Este), AWS GovCloud (EEUU-Oeste) y China (Ningxia)

Parámetros:

deleteOnTermination (Opcional), Tipo: booleano

> Los volúmenes de EBS se marcan para eliminarse cuando se termina una instancia. Valores posibles: True o False (los demás valores de entrada se marcan como NON_COMPLIANT) Si se establece en `True`, la regla es NON_COMPLIANT si un volumen de EBS terminado no está marcado para su eliminación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 vpn-connection-logging-enabled

Comprueba si las conexiones AWS Site-to-Site VPN tienen habilitado el CloudWatch registro de Amazon para ambos túneles. La regla no cumple con los requisitos si una conexión Site-to-Site VPN no tiene habilitado el CloudWatch registro en ninguno de los túneles o en ambos.

Identificador: _VPN_CONNECTION_LOGGING_ENABLED EC2

Tipos de recursos: AWS::EC2::VPNConnection

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 vpn-connection-tagged

Comprueba si las conexiones de Amazon EC2 VPN tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EC2 _VPN_CONNECTION_TAGGED

Tipos de recursos: AWS::EC2::VPNConnection

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecr-private-image-scanning-habilitado

Comprueba si un repositorio de Amazon Elastic Container Registry (Amazon ECR) tiene habilitado el escaneo de imágenes. La regla es NON_COMPLIANT si la frecuencia de escaneo del repositorio de Amazon ECR privado no es la misma que la del escaneo automático o continuo. Para obtener más información sobre la habilitación del escaneo de imágenes, consulte Escaneo de imágenes en la Guía del usuario de Amazon ECR.

Identificador: ECR_PRIVATE_IMAGE_SCANNING_ENABLED

Tipos de recursos: AWS::ECR::Repository

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecr-private-lifecycle-policy-configurado

Comprueba si un repositorio privado de Amazon Elastic Container Registry (ECR) tiene configurada al menos una política de ciclo de vida. La regla es NON_COMPLIANT si no se ha configurado ninguna política de ciclo de vida para el repositorio privado de ECR.

Identificador: ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

Tipos de recursos: AWS::ECR::Repository

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ecr-private-tag-immutability-habilitado

Comprueba si un repositorio de Amazon Elastic Container Registry (ECR) tiene habilitada la inmutabilidad de las etiquetas. Esta regla es NON_COMPLIANT si la inmutabilidad de etiquetas no está habilitada para el repositorio de ECR privado.

Identificador: ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

Tipos de recursos: AWS::ECR::Repository

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecr-repository-cmk-encryption-habilitado

Comprueba si el repositorio de ECR está cifrado en reposo mediante una clave de KMS administrada por el cliente. Esta regla NO CUMPLE con los requisitos si el repositorio se cifra con la clave KMS predeterminada ('aws/ecr') AES256 o con la clave KMS predeterminada.

Identificador: ECR_REPOSITORY_CMK_ENCRYPTION_ENABLED

Tipos de recursos: AWS::ECR::Repository

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

> Lista separada por comas de Amazon Resource Names (ARNs) con clave de KMS destinada a cifrar el repositorio de ECR.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecr-repository-tagged

Comprueba si los repositorios de Amazon ECR tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: ECR_REPOSITORY_TAGGED

Tipos de recursos: AWS::ECR::Repository

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ecs-awsvpc-networking-enabled

Comprueba si el modo de red de las definiciones activas ECSTask está establecido en «awsvpc». Esta regla NO CUMPLE CON LOS REQUISITOS si las ECSTask definiciones activas no están configuradas en «awsvpc».

> **Note**
>
> Esta regla solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

AWSVPC_NETWORKINGIdentificador: ECS_ _ENABLED

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ecs-capacity-provider-tagged

Comprueba si los proveedores de capacidad de Amazon ECS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: ECS_CAPACITY_PROVIDER_TAGGED

Tipos de recursos: AWS::ECS::CapacityProvider

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-capacity-provider-termination-comprobar

Comprueba si un proveedor de Amazon ECS Capacity que contiene grupos de Auto Scaling ha activado la protección de terminación administrada. Esta regla NO CUMPLE CON LOS REQUISITOS si la protección de terminación gestionada está desactivada en el proveedor de capacidad de ECS.

Identificador: ECS_CAPACITY_PROVIDER_TERMINATION_CHECK

Tipos de recursos: AWS::ECS::CapacityProvider

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-containers-nonprivileged

Comprueba si el parámetro privilegiado de la definición del contenedor de ECSTask las definiciones está establecido en «verdadero». La regla es NON_COMPLIANT si el parámetro privilegiado es true.

> **Note**
>
> Esta regla solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Identificador: ECS_CONTAINERS_NONPRIVILEGED

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-containers-readonly-access

Comprueba si los contenedores de Amazon Elastic Container Service (Amazon ECS) solo tienen acceso de solo lectura a sus sistemas de archivos raíz. La regla no cumple con los requisitos si el readonlyRootFilesystem parámetro de la definición del contenedor de las definiciones está establecido en «falso». ECSTask

> **Note**
>
> Esta regla solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Identificador: ECS_CONTAINERS_READONLY_ACCESS

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-container-insights-enabled

Comprueba si los clústeres de Amazon Elastic Container Service tienen habilitada la información sobre contenedores. La regla es NON_COMPLIANT si la información del contenedor no está habilitada.

Identificador: ECS_CONTAINER_INSIGHTS_ENABLED

Tipos de recursos: AWS::ECS::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-fargate-latest-platform-versión

Comprueba si los servicios de ECS Fargate están configurados con la última versión de la plataforma. La regla no es compatible si el tipo PlatformVersion de lanzamiento de Fargate no está establecido en LATEST o si no se proporciona latestLinuxVersion ni `latestWindowsVersion` se proporciona como parámetro.

Identificador: ECS_FARGATE_LATEST_PLATFORM_VERSION

Tipos de recursos: AWS::ECS::Service

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

latestLinuxVersion (Opcional), Tipo: cadena

La última versión de Linux admite 'PlatformVersion' en formato de versionado semántico (SemVer). El parámetro puede ser necesario si Fargate se implementó y el 'PlatformVersion' se especificó explícitamente o CodeDeploy se usa como '' DeploymentController

latestWindowsVersion (Opcional), Tipo: cadena

La última versión de Windows admitía PlatformVersion '' en formato de versionado semántico (SemVer). El parámetro puede ser necesario si Fargate se implementó y el 'PlatformVersion' se especificó explícitamente o CodeDeploy se usa como '' DeploymentController

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ecs-no-environment-secrets

Comprueba si los secretos se transmiten como variables de entorno del contenedor. La regla es NON_COMPLIANT si una o más claves de variables de entorno coinciden con una clave incluida en el parámetro `secretKeys` (excluidas las variables de entorno de otras ubicaciones, como Amazon S3).

> **Note**
>
> Esta regla solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Identificador: ECS_NO_ENVIRONMENT_SECRETS

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

secretKeys, Tipo: CSV

> Lista de nombres clave separados por comas para buscarlos en las variables de entorno de las definiciones de contenedor dentro de las definiciones de tareas. Se eliminarán los espacios adicionales.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ecs-task-definition-efs-cifrado activado

Comprueba si las definiciones de tareas de Amazon ECS con volúmenes EFS tienen activado el cifrado en tránsito. La regla no es compatible si una definición de tarea de ECS contiene un volumen EFS sin el cifrado de tránsito activado.

Identificador: ECS_TASK_DEFINITION_EFS_ENCRYPTION_ENABLED

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-task-definition-linux-user-non-root

Comprueba si la última revisión activa de una definición de tarea de Amazon ECS configura los contenedores de Linux para que se ejecuten como usuarios no root. La regla es NON_COMPLIANT si se especifica el usuario root o no hay configuración de usuario para ningún contenedor.

Identificador: ECS_TASK_DEFINITION_LINUX_USER_NON_ROOT

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-task-definition-log-configuración

Comprueba si logConfiguration está establecido en las definiciones de tareas activas de Amazon ECS. Esta regla no cumple con los requisitos si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

> **Note**
>
> Esta regla solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Identificador: ECS_TASK_DEFINITION_LOG_CONFIGURATION

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ecs-task-definition-memory-límite estricto

Comprueba si las definiciones de tareas de Amazon Elastic Container Service (ECS) tienen un límite de memoria establecido para las definiciones de contenedor. La regla es NON_COMPLIANT para una definición de tarea si el parámetro memory no está presente en una definición de contenedor.

> **Note**
>
> Esta regla solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Identificador: ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico

(Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-task-definition-network-mode-not-host

Comprueba si la última revisión activa de las definiciones de tarea de Amazon ECS utiliza el modo de red de host. La regla es NON_COMPLIANT si la última revisión activa de la definición de tarea de ECS utiliza el modo de red de host.

Identificador: ECS_TASK_DEFINITION_NETWORK_MODE_NOT_HOST

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-task-definition-nonroot-usuario

Comprueba si ECSTask las definiciones especifican un usuario en el que se ejecutarán los contenedores del tipo de lanzamiento de Amazon Elastic Container Service (Amazon EC2 ECS). La regla es NON_COMPLIANT si el parámetro User no está presente o está establecido en Root.

> **Note**
>
> Esta regla solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Identificador: ECS_TASK_DEFINITION_NONROOT_USER

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ecs-task-definition-pid-comprobación de modo

Comprueba si ECSTask las definiciones están configuradas para compartir el espacio de nombres de procesos de un host con sus contenedores de Amazon Elastic Container Service (Amazon ECS). La regla es NON_COMPLIANT si el parámetro pidMode está establecido en host.

> **Note**
>
> Esta regla solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Identificador: ECS_TASK_DEFINITION_PID_MODE_CHECK

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ecs-task-definition-user-for-host-mode-check

Comprueba si las definiciones de tareas de Amazon ECS con el modo de red de host tienen “privileged” o “nonroot” en la definición del contenedor. La regla es NON_COMPLIANT si la última revisión activa de una definición de tarea tiene privileged=false (o es nulo) Y user=root (o es nulo).

> **Important**
>
> Solo se debe cumplir una condición para que la regla devuelva conformidad
> La regla es COMPLIANT en cualquiera de los siguientes escenarios:
>
> - Si el modo de red no está configurado como host.
> - Si la última revisión activa de una definición de tarea tiene privileged=true.
> - Si la última revisión activa de una definición de tarea tiene un usuario que no es root.
>
> Esto significa que solo se debe cumplir una de estas condiciones para que la regla devuelva conformidad. Para comprobar específicamente si una definición de tarea tiene privileged=true, consulte. [ecs-containers-nonprivileged](#) [Para comprobar específicamente si una definición de tarea tiene un usuario que no es el root, consulte -user. ecs-task-definition-nonroot](#)

Identificador: ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

SkipInactiveTaskDefinitions (Opcional), Tipo: booleano

> Indicador booleano para no comprobar las definiciones de EC2 tareas de Amazon INACTIVAS. Si se establece en «true», la regla no evaluará las definiciones de EC2 tareas de Amazon INACTIVAS. Si se establece en «false», la regla evaluará la última revisión de las definiciones de EC2 tareas de Amazon INACTIVAS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ecs-task-definition-windows-user-non-admin

Comprueba si la última revisión activa de una definición de tarea de Amazon ECS configura los contenedores de Windows para que se ejecuten como usuarios no administradores. La regla no cumple con los requisitos si se especifica un usuario administrador predeterminado o si no hay ninguna configuración de usuario en algún contenedor.

Identificador: ECS_TASK_DEFINITION_WINDOWS_USER_NON_ADMIN

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

efs-access-point-enforce-directorio-raíz

Comprueba si los puntos de acceso de Amazon Elastic File System (Amazon EFS) están configurados para forzar un directorio raíz. La regla es NON_COMPLIANT si el valor de Path se establece en / (directorio raíz predeterminado del sistema de archivos).

Identificador: EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

Tipos de recursos: AWS::EFS::AccessPoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

approvedDirectories (opcional), Tipo: CSV

> Lista separada por comas de las rutas de subdirectorios que están aprobadas para la aplicación del directorio raíz de los puntos de acceso de Amazon EFS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

efs-access-point-enforce-identidad de usuario

Comprueba si los puntos de acceso de Amazon Elastic File System (Amazon EFS) están configurados para aplicar una identidad de usuario. La regla no es compatible si 'PosixUser' no está definido o si se proporcionan parámetros y no hay coincidencia en el parámetro correspondiente.

Identificador: EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

Tipos de recursos: AWS::EFS::AccessPoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

approvedUids (opcional), Tipo: CSV

Lista separada por comas de los ID de usuario POSIX aprobados para la aplicación de usuarios del punto de acceso de EFS.

approvedGids (opcional), Tipo: CSV

Lista separada por comas de los grupos IDs POSIX aprobados para la aplicación por parte de los usuarios de los puntos de acceso EFS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

efs-automatic-backups-enabled

Comprueba si un sistema de archivos de Amazon Elastic File System (Amazon EFS) tiene habilitadas las copias de seguridad automáticas. La regla no es compatible si `.Status` se establece en DESHABILITADO. BackupPolicy

Identificador: EFS_AUTOMATIC_BACKUPS_ENABLED

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

efs-encrypted-check

Comprueba si Amazon Elastic File System (Amazon EFS) está configurado para cifrar los datos del archivo mediante AWS Key Management Service (AWS KMS). La regla es NON_COMPLIANT si la clave cifrada está establecida en false en `DescribeFileSystems` o si la clave de `KmsKeyId` en `DescribeFileSystems` no coincide con el parámetro `KmsKeyId`.

Identificador: EFS_ENCRYPTED_CHECK

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

KmsKeyId (Opcional), Tipo: cadena

> Nombre de recurso de Amazon (ARN) de la clave de KMS que se utiliza para cifrar el sistema de archivos de EFS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

efs-filesystem-ct-encrypted

Comprueba si Amazon Elastic File System (Amazon EFS) cifra los datos con AWS Key Management Service (AWS KMS). La regla es NON_COMPLIANT si hay un sistema de archivos que no está cifrado. Si lo desea, puede comprobar si hay un sistema de archivos que no esté cifrado con claves KMS específicas.

Identificador: EFS_FILESYSTEM_CT_ENCRYPTED

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

kmsKeyArns (Opcional), Tipo: cadena

(Opcional) Lista separada por comas de nombres de recursos de Amazon (ARNs) para claves de AWS KMS. Si se proporciona, la regla comprueba si las claves de KMS especificadas no cifran un sistema de archivos de Amazon EFS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

efs-file-system-tagged

Comprueba si los sistemas de archivos de Amazon Elastic File System tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EFS_FILE_SYSTEM_TAGGED

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

efs-in-backup-plan

Comprueba si los sistemas de archivos Amazon Elastic File System (Amazon EFS) se han añadido a los planes de AWS backup de Backup. La regla es NON_COMPLIANT si los sistemas de archivos de EFS no están incluidos en los planes de copia de seguridad.

Identificador: EFS_IN_BACKUP_PLAN

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

efs-last-backup-recovery-punto creado

Comprueba si se ha creado un punto de recuperación para el sistema de archivos de Amazon Elastic File System (Amazon EFS). La regla es NON_COMPLIANT si el sistema de archivos de EFS no tiene ningún punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los sistemas de archivos de Amazon EFS para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID del sistema de archivos de EFS para que la regla lo compruebe.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

efs-meets-restore-time-objetivo

Comprueba si el tiempo de restauración de los sistemas de archivos de Amazon Elastic File System (Amazon EFS) cumple con la duración especificada. La regla es NON_COMPLIANT si el LatestRestoreExecutionTimeMinutes tamaño de un sistema de archivos Amazon EFS es superior maxRestoreTime a minutos.

Identificador: EFS_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

maxRestoreTime, Tipo: int

Valor numérico del tiempo de ejecución de restauración máximo permitido.

resourceTags (opcional), Tipo: cadena

Etiquetas de los sistemas de archivos de Amazon EFS para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID del sistema de archivos de EFS para que la regla lo compruebe.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

efs-mount-target-public-accesible

Comprueba si hay un Amazon Elastic File System (Amazon EFS) que está asociado a subredes que asignan direcciones IP públicas en el momento del lanzamiento. La regla es NON-COMPLIANT si el destino de montaje de Amazon EFS está asociado a subredes que asignan direcciones IP públicas en el inicio.

Identificador: EFS_MOUNT_TARGET_PUBLIC_ACCESSIBLE

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

efs-resources-in-logically-air-gapped-vault

Comprueba si los sistemas de archivos de Amazon Elastic File System (Amazon EFS) están dentro de un almacén aislado lógicamente. La regla es NON_COMPLIANT si hay una sistema de archivos de Amazon EFS que no está en un almacén aislado lógicamente dentro del período de tiempo especificado.

Identificador: EFS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

resourceTags (opcional), Tipo: cadena

> Etiquetas de los sistemas de archivos de Amazon EFS para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID del sistema de archivos de EFS para que la regla lo compruebe.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 2184 horas y 91 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

efs-resources-protected-by-plan de respaldo

Comprueba si los sistemas de archivos de Amazon Elastic File System (Amazon EFS) están protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el sistema de archivos de EFS no está cubierto por un plan de copia de seguridad.

Identificador: EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::EFS::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas para los sistemas de archivos de EFS para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID del sistema de archivos de EFS para que la regla los compruebe.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

eip-attached

Comprueba si todas las direcciones IP elásticas que se asignan a una AWS cuenta están conectadas a EC2 instancias o interfaces de red elásticas en uso. La regla NO CUMPLE CON LOS REQUISITOS si el valor 'AssociationId' es nulo para la dirección IP elástica.

> **Note**
>
> Los resultados pueden tardar hasta 6 horas en estar disponibles después de que se produzca una evaluación.

Identificador: EIP_ATTACHED

Tipos de recursos: AWS::EC2::EIP

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con AWS Config reglas. Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

eks-addon-tagged

Comprueba si los complementos de Amazon EKS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EKS_ADDON_TAGGED

Tipos de recursos: AWS::EKS::Addon

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

eks-cluster-logging-enabled

Comprueba si un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) está configurado con el registro activado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitado para todos los tipos de registro.

Identificador: EKS_CLUSTER_LOGGING_ENABLED

Tipos de recursos: AWS::EKS::Cluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

eks-cluster-log-enabled

Comprueba si un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) está configurado con el registro activado. La regla es NON_COMPLIANT si el registro para los clústeres de Amazon EKS no está habilitado o si el registro no está habilitado con el tipo de registro mencionado.

Identificador: EKS_CLUSTER_LOG_ENABLED

Tipos de recursos: AWS::EKS::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

logTypes (opcional), Tipo: CSV

> Lista separada por comas de los tipos de registro de plano de control de clúster de EKS que la regla debe cumplir. Valores válidos: “api”, “audit”, “authenticator”, “controllerManager”, “scheduler”

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

eks-cluster-oldest-supported-versión

Comprueba si un clúster de Amazon Elastic Kubernetes Service (EKS) ejecuta la versión compatible más antigua. La regla es NON_COMPLIANT si un clúster de EKS ejecuta la versión compatible más antigua (igual al parámetro `oldestVersionSupported`).

Identificador: EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

Tipos de recursos: AWS::EKS::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

oldestVersionSupported, Tipo: cadena

Valor de la versión más antigua de Kubernetes compatible con AWS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

eks-cluster-secrets-encrypted

Comprueba si los clústeres de Amazon EKS están configurados para cifrar los secretos de Kubernetes mediante KMS. AWS La regla es NON_COMPLIANT si hay un clúster de EKS sin un recurso de encryptionConfig o si encryptionConfig no designa secretos como un recurso.

Identificador: EKS_CLUSTER_SECRETS_ENCRYPTED

Tipos de recursos: AWS::EKS::Cluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

Lista separada por comas de los nombres de recursos de Amazon (ARNs) clave de KMS aprobados para su uso en EKS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

eks-cluster-supported-version

Comprueba si un clúster de Amazon Elastic Kubernetes Service (EKS) ejecuta una versión de Kubernetes compatible. Esta regla es NON_COMPLIANT si un clúster de EKS ejecuta una versión no compatible (inferior al parámetro `oldestVersionSupported`).

Identificador: EKS_CLUSTER_SUPPORTED_VERSION

Tipos de recursos: AWS::EKS::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

oldestVersionSupported, Tipo: cadena

Valor de la versión más antigua de Kubernetes compatible con AWS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

eks-endpoint-no-public-acceso

Comprueba si el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no es de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.

Identificador: EKS_ENDPOINT_NO_PUBLIC_ACCESS

Tipos de recursos: AWS::EKS::Cluster

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

eks-fargate-profile-tagged

Comprueba si los perfiles fargate de Amazon EKS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EKS_FARGATE_PROFILE_TAGGED

Tipos de recursos: AWS::EKS::FargateProfile

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

eks-secrets-encrypted

Comprueba si los clústeres de Amazon Elastic Kubernetes Service están configurados para cifrar los secretos de Kubernetes mediante claves (KMS). AWS Key Management Service

- Esta regla es COMPLIANT si un clúster de EKS tiene una encryptionConfig con secretos como uno de los recursos.
- Esta regla también es COMPLIANT si la clave utilizada para cifrar los secretos de EKS coincide con el parámetro.
- Esta regla es NON_COMPLIANT si un clúster de EKS no tiene una encryptionConfig o si los recursos de encryptionConfig no incluyen secretos.
- Esta regla también es NON_COMPLIANT si la clave utilizada para cifrar los secretos de EKS no coincide con el parámetro.

Identificador: EKS_SECRETS_ENCRYPTED

Tipos de recursos: AWS::EKS::Cluster

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

> Lista separada por comas de los nombres de recurso de Amazon (ARN) de la clave de KMS que debe utilizarse para cifrar los secretos en un clúster de EKS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticache-automatic-backup-check-habilitado

Comprueba si ElastiCache los clústeres de Amazon (Valkey o Redis OSS) tienen activada la copia de seguridad automática. La regla no cumple con los requisitos si la copia de seguridad automática no está habilitada o si el valor SnapshotRetentionLimit de un clúster es inferior al especificado. `snapshotRetentionPeriod`

Identificador: ELASTICACHE_AUTOMATIC_BACKUP_CHECK_ENABLED

Tipos de recursos: AWS::ElastiCache::CacheCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

snapshotRetentionPeriod (Opcional), Tipo: int

> Período mínimo de retención de instantáneas en días para Valkey o Redis OSS. Los valores válidos están comprendidos entre 1 y 35. El valor predeterminado es 1.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elasticache-auto-minor-version-verificación de actualizaciones

Comprueba si ElastiCache los clústeres de Amazon tienen habilitadas las actualizaciones automáticas de las versiones secundarias. La regla no cumple con los requisitos para un ElastiCache clúster si utiliza el motor Redis o Valkey y '' no está configurado como AutoMinorVersionUpgrade 'true'.

Identificador: ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

Tipos de recursos: AWS::ElastiCache::CacheCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Región Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elasticache-rbac-auth-enabled

Comprueba si los grupos de ElastiCache replicación de Amazon tienen habilitada la autenticación RBAC. La regla no cumple con los requisitos si la versión de Redis es 6 o superior y falta 'UserGroupIds', está vacía o no coincide con una entrada proporcionada por el parámetro ''. `allowedUserGroupIDs`

Identificador: ELASTICACHE_RBAC_AUTH_ENABLED

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

allowedUserGroupIDs (Opcional), Tipo: CSV

> Lista separada por comas de los grupos de usuarios aprobados para IDs el acceso a los grupos de ElastiCache replicación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticache-redis-cluster-automatic-verificación de respaldo

Compruebe si los clústeres de Amazon ElastiCache Redis tienen activada la copia de seguridad automática. La regla no es compatible si el clúster SnapshotRetentionLimit de Redis es inferior al parámetro. SnapshotRetentionPeriod Por ejemplo: si el parámetro es 15, la regla no es compatible si está entre 0 y 15. snapshotRetentionPeriod

Identifier (Identificador): ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

Tipos de recursos:, AWS::ElastiCache::CacheCluster AWS::ElastiCache::ReplicationGroup

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles, excepto la región de Asia Pacífico (Taipéi)

Parámetros:

snapshotRetentionPeriod (Opcional), Tipo: int, Valor predeterminado: 15

> Período mínimo de retención de instantáneas en días para el clúster de Redis. El valor predeterminado es 15 días.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticache-repl-grp-auto-habilitado para conmutación por error

Comprueba si los grupos de replicación de Amazon ElastiCache Redis tienen habilitada la conmutación por error automática. La regla no cumple con los requisitos para un grupo de ElastiCache replicación si '' no está configurado como AutomaticFailover 'activado'.

Identificador: ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Región Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elasticache-repl-grp-encrypted-en reposo

Comprueba si los grupos de ElastiCache replicación de Amazon están encryption-at-rest habilitados. La regla no es compatible para un grupo de ElastiCache replicación si 'AtRestEncryptionEnabled' está deshabilitado o si el ARN de la clave KMS no coincide con el parámetro Arns aprobado. KMSKey

Identificador: ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Región Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

KMSKeyIdentificaciones aprobadas (opcionales), Tipo: CSV

Lista separada por comas de las claves de KMS IDs cuyo uso está aprobado. ElastiCache

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticache-repl-grp-encrypted-en tránsito

Comprueba si los grupos de ElastiCache replicación de Amazon están encryption-in-transit habilitados. La regla no cumple con los requisitos para un grupo de ElastiCache replicación si «TransitEncryptionEnabled» está configurado como «falso».

Identificador: ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Región Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticache-repl-grp-redis-habilitada para autenticación

Comprueba si los grupos de ElastiCache replicación de Amazon tienen habilitada la autenticación de Redis. La regla no cumple con los requisitos para un grupo de ElastiCache replicación si la versión de Redis de sus nodos es inferior a 6 (la versión 6+ usa Redis ACLs) y falta " AuthToken o está vacía/nula.

Identificador: ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Zúrich)) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elasticache-subnet-group-check

Comprueba si ElastiCache los clústeres de Amazon están configurados con un grupo de subredes personalizado. La regla no es conforme para un ElastiCache clúster si utiliza un grupo de subredes predeterminado.

Identificador: ELASTICACHE_SUBNET_GROUP_CHECK

Tipos de recursos: AWS::ElastiCache::CacheCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticache-supported-engine-version

Comprueba si ElastiCache los clústeres ejecutan una versión superior o igual a la versión de motor recomendada. La regla no cumple con los requisitos si el valor 'EngineVersion' de un ElastiCache clúster es inferior a la versión recomendada especificada para el motor correspondiente.

Identificador: ELASTICACHE_SUPPORTED_ENGINE_VERSION

Tipos de recursos: AWS::ElastiCache::CacheCluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Centro), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

latestMemcachedVersion, Tipo: cadena

> Última versión de motor recomendada para Memcached. Los valores válidos están en formato de versionado semántico (SemVer) con un número de 3 componentes para las versiones principal, secundaria y de parche (por ejemplo, 1.6.6, no 1.6).

latestRedisVersion, Tipo: cadena

> Última versión de motor recomendada para Redis. Los valores válidos están en formato de versionado semántico (SemVer) con números de 3 componentes para las versiones principales, secundarias y de parche (por ejemplo, 7.0.5, no 7.0).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticbeanstalk-application-description

Comprueba si las aplicaciones de AWS Elastic Beanstalk tienen una descripción. La regla es NON_COMPLIANT si configuration.description no existe o es una cadena vacía.

Identificador: ELASTICBEANSTALK_APPLICATION_DESCRIPTION

Tipos de recursos: AWS::ElasticBeanstalk::Application

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elasticbeanstalk-application-version-description

Comprueba si AWS las versiones de la aplicación Elastic Beanstalk tienen una descripción. La regla es NON_COMPLIANT si configuration.description no existe o es una cadena vacía.

Identificador: ELASTICBEANSTALK_APPLICATION_VERSION_DESCRIPTION

Tipos de recursos: AWS::ElasticBeanstalk::ApplicationVersion

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico

(Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticbeanstalk-environment-description

Comprueba si los entornos de AWS Elastic Beanstalk tienen una descripción. La regla es NON_COMPLIANT si configuration.description no existe o es una cadena vacía.

Identificador: ELASTICBEANSTALK_ENVIRONMENT_DESCRIPTION

Tipos de recursos: AWS::ElasticBeanstalk::Environment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticsearch-encrypted-at-rest

Comprueba si los dominios OpenSearch de Amazon Service (anteriormente denominados Elasticsearch) tienen habilitada la configuración de cifrado en reposo. La regla no es compatible si el EncryptionAtRestOptions campo no está activado.

Identificador: ELASTICSEARCH_ENCRYPTED_AT_REST

Tipos de recursos: AWS::Elasticsearch::Domain

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elasticsearch-in-vpc-only

Comprueba si los dominios OpenSearch de Amazon Service (anteriormente denominados Elasticsearch) están en Amazon Virtual Private Cloud (Amazon VPC). La regla no cumple con los requisitos si el punto final de un dominio de OpenSearch servicio es público.

Identificador: ELASTICSEARCH_IN_VPC_ONLY

Tipos de recursos: AWS::Elasticsearch::Domain

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticsearch-logs-to-cloudwatch

Comprueba si los dominios OpenSearch de servicio (anteriormente denominados Elasticsearch) están configurados para enviar registros a CloudWatch Logs. La regla cumple con las normas si hay un registro habilitado para un dominio de OpenSearch servicio. La regla es NON_COMPLIANT si el registro no está configurado.

Identificador: ELASTICSEARCH_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::Elasticsearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

logTypes (opcional), Tipo: CSV

> Lista separada por comas de los registros que están habilitados. Los valores válidos son «búsqueda», «índice» y «error»

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con AWS Config reglas. Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
```

```
...
```

*Objeto con una o varias de las claves siguientes: `SEARCH_SLOW_LOGS`, `ES_APPLICATION_LOGS`, `INDEX_SLOW_LOGS` o `AUDIT_LOGS`, según los tipos de registros que desee publicar. Cada clave necesita un valor `LogPublishingOption` válido.

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elasticsearch-node-to-node-comprobación de cifrado

Comprueba que los nodos OpenSearch de Amazon Service estén cifrados de extremo a extremo. La regla no cumple con los requisitos si el node-to-node cifrado está deshabilitado en el dominio.

Identificador: ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Tipos de recursos: AWS::Elasticsearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con reglas. AWS Config Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
```

```
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elastic-beanstalk-logs-to- vigilancia en la nube

Comprueba si los entornos de AWS Elastic Beanstalk están configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

Identificador: ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::ElasticBeanstalk::Environment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

RetentionInDays (Opcional), Tipo: cadena

> Comprueba el número de días que se van a conservar los eventos de registro antes de que expiren. Los valores válidos son 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827 y 3653. La regla es NON_COMPLIANT si el valor de `logs. RetentionInDays`no coincide con este parámetro.

DeleteOnTerminate (Opcional), Tipo: cadena

> Comprueba si los registros están configurados para eliminarse al finalizar el entorno. Los valores válidos son true o false. La regla es NON_COMPLIANT si el valor de `logs. DeleteOnTerminate`no coincide con este parámetro.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elastic-beanstalk-managed-updates-habilitado

Comprueba si las actualizaciones de plataforma gestionadas en un AWS Elastic Beanstalk entorno están habilitadas. La regla es COMPLIANT si el valor de `ManagedActionsEnabled` se establece en true. La regla es NON_COMPLIANT si el valor de `ManagedActionsEnabled` se define como false o si se proporciona un parámetro cuyo valor no coincide con las configuraciones existentes.

Identificador: ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

Tipos de recursos: AWS::ElasticBeanstalk::Environment

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Hyderabad), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y Europa (Zúrich)

Parámetros:

UpdateLevel (Opcional), Tipo: cadena

> Indica si los niveles de actualización están configurados con actualizaciones de versiones secundarias o de parches.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elb 2- acm-certificate-required

Comprueba si los balanceadores de carga de aplicaciones y los balanceadores de carga de red tienen oyentes configurados para usar certificados de (ACM). AWS Certificate Manager Esta regla es NON_COMPLIANT si al menos un equilibrador de carga tiene como mínimo un oyente configurado sin un certificado de ACM o está configurado con un certificado que no es de ACM.

ELBV2Identificador: _ACM_CERTIFICATE_REQUIRED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), Región de Europa (Zúrich)

Parámetros:

AcmCertificatesAllowed (Opcional), Tipo: CSV

Lista de certificados separados por comas de Amazon Resource Names ()ARNs.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elb 2- listener-encryption-in-transit

Comprueba si los oyentes de los equilibradores de carga están configurados con una terminación HTTPS o TLS. La regla es NON_COMPLIANT si no hay oyentes configurados con una terminación HTTP o TLS.

Identificador: _LISTENER_ENCRYPTION_IN_TRANSIT ELBV2

Tipos de recursos: AWS::ElasticLoadBalancingV2::Listener

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elbv2-multiple-az

Comprueba si un Elastic Load Balancer V2 (balanceador de carga de aplicaciones, redes o puertas de enlace) está mapeado a varias zonas de disponibilidad (). AZs La regla no cumple con las normas si un Elastic Load Balancer V2 está asignado a menos de 2. AZs Para obtener más información, consulte Zonas de disponibilidad del equilibrador de carga de aplicación.

ELBV2Identificador: _MULTIPLE_AZ

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

minAvailabilityZones (Opcional), Tipo: int

Número mínimo esperado AZs (entre 2 y 10 inclusive).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elbv2- -check predefined-security-policy-ssl

Comprueba si los oyentes de los balanceadores de carga de aplicaciones (ALBs) o los balanceadores de carga de red () utilizan determinadas políticas de seguridad. NLBs La regla es NON_COMPLIANT si un oyente de HTTPS para un ALB o un oyente de TLS para un NLB no utiliza las políticas de seguridad que usted especifique.

Identificador: _PREDEFINED_SECURITY_POLICY_SSL_CHECK ELBV2

Tipos de recursos: AWS::ElasticLoadBalancingV2::Listener

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningun Xia), Región de Europa (Zúrich)

Parámetros:

sslPolicies, Tipo: CSV

> Lista separada por comas de políticas de seguridad que la regla debe comprobar. Por ejemplo, "ELBSecurityPolicy- TLS13 -1-2-2021-06".

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elb-acm-certificate-required

Comprueba si los balanceadores de carga clásicos utilizan los certificados SSL proporcionados por. AWS Certificate Manager Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Esta regla solo se aplica a los Classic Load Balancers. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

Identificador: ELB_ACM_CERTIFICATE_REQUIRED

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto África (Ciudad del Cabo), Asia Pacífico (Osaka), Europa (Milán), Israel (Tel Aviv), Canadá Oeste (Calgary), Europa (España) y Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elb-cross-zone-load-habilitado para el equilibrio

Comprueba si el equilibrio de carga entre zonas está habilitado para los equilibradores de carga clásicos. La regla es NON_COMPLIANT si el equilibrio de carga entre zonas no está habilitado para los equilibradores de carga clásicos.

Identificador: ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elb-custom-security-policy-comprobación de SSL

Comprueba si los oyentes SSL de su equilibrador de carga clásico utilizan una política personalizada. La regla solo se aplica si hay oyentes SSL para el equilibrador de carga clásico.

Identificador: ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

sslProtocolsAndCifrados, Tipo: CSV

Lista separada por comas de cifrados y protocolos.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elb-deletion-protection-enabled

Comprueba si un equilibrador de carga elástico tiene habilitada la protección contra eliminación. La regla es NON_COMPLIANT si deletion_protection.enabled está definido como false.

Identificador: ELB_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elb-internal-scheme-check

Comprueba si un esquema del equilibrador de carga clásico es interno. La regla es NON_COMPLIANT si el esquema de configuración no se establece como interno.

Identificador: ELB_INTERNAL_SCHEME_CHECK

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elb-logging-enabled

Comprueba si el equilibrador de carga de aplicación y el equilibrador de carga clásico tienen habilitado el registro. La regla es NON_COMPLIANT si `access_logs.s3.enabled` es falsa o no `access_logs.S3.bucket` es igual al s3 BucketName que ha proporcionado.

> **Note**
>
> La regla no se aplica a los equilibradores de carga de red ni a los equilibradores de carga de puerta de enlace.

Identificador: ELB_LOGGING_ENABLED

Tipos de recursos:, AWS::ElasticLoadBalancing::LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

s3 BucketNames (opcional), Tipo: CSV

Lista separada por comas de nombres de bucket de Amazon S3 para que Amazon ELB entregue los archivos de registro.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elb-predefined-security-policy-comprobación de SSL

Comprueba si los oyentes SSL de su equilibrador de carga clásico utilizan la política predefinida. La regla no es compatible si la política del listener de Classic Load HTTPS/SSL Balancer no es igual al valor del parámetro ". `predefinedPolicyName`

Identificador: ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

predefinedPolicyName, Tipo: cadena

Nombre de la política predefinida.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

elb-tagged

Comprueba si los equilibradores de carga clásicos tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: ELB_TAGGED

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

elb-tls-https-listeners-solo

Comprueba si el equilibrador de carga clásico está configurado con oyentes SSL o HTTPS. La regla es NON_COMPLIANT si un oyente no está configurado con SSL o HTTPS.

- Si el equilibrador de carga clásico no tiene un oyente configurado, la regla devuelve `NOT_APPLICABLE`.
- La regla es COMPLIANT si los oyentes del equilibrador de carga clásico se configuran con SSL o HTTPS.

- La regla es NON_COMPLIANT si un oyente no está configurado con SSL o HTTPS.

Identificador: ELB_TLS_HTTPS_LISTENERS_ONLY

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

emr-block-public-access

Comprueba si una cuenta de Amazon EMR tiene habilitada la configuración de bloqueo de acceso público. La regla no cumple con los requisitos si BlockPublicSecurityGroupRules es falsa o, si es verdadera, los puertos distintos del puerto 22 aparecen en la lista. PermittedPublicSecurityGroupRuleRanges

Identificador: EMR_BLOCK_PUBLIC_ACCESS

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

emr-kerberos-enabled

Comprueba que los clústeres de Amazon EMR tengan Kerberos habilitado. La regla es NON_COMPLIANT si no hay asociada una configuración de seguridad al clúster o si la configuración de seguridad no cumple los parámetros de regla especificados.

Identifier (Identificador): EMR_KERBEROS_ENABLED

Tipos de recursos: AWS::EMR::Cluster

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

TicketLifetimeInHours (Opcional), Tipo: int

Período durante el que es válido el ticket Kerberos emitido por el KDC del clúster.

Realm (opcional), Tipo: cadena

Nombre de ámbito de Kerberos del otro ámbito en la relación de confianza.

Domain (opcional), Tipo: cadena

Nombre de dominio del otro ámbito en la relación de confianza.

AdminServer (Opcional), Tipo: cadena

Nombre de dominio completo (FQDN) del servidor de administración del otro ámbito de la relación de confianza.

KdcServer (Opcional), Tipo: cadena

Nombre de dominio completo (FQDN) del servidor de KDC en el otro ámbito de la relación de confianza.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

emr-master-no-public-IP

Comprueba si los nodos maestros de los clústeres de Amazon EMR son públicos. IPs La regla es NON_COMPLIANT si el nodo maestro tiene una IP pública.

> **Note**
>
> Esta regla comprueba los clústeres que están en estado RUNNING o WAITING. Esta regla requiere que habilite el registro para el tipo de recurso `AWS::EC2::Instance` a fin de tener una evaluación precisa.

Identifier (Identificador): EMR_MASTER_NO_PUBLIC_IP

Tipos de recursos:, AWS::EMR::Cluster AWS::EC2::Instance

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

emr-security-configuration-encryption-descanso

Comprueba si la configuración de seguridad de Amazon EMR tiene habilitado el cifrado en reposo. La regla no cumple con las normas si está configurada. SecurityConfiguration. EncryptionConfiguration. EnableAtRestEncryption es falso.

Identificador: EMR_SECURITY_CONFIGURATION_ENCRYPTION_REST

Tipos de recursos: AWS::EMR::SecurityConfiguration

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

emr-security-configuration-encryption-tránsito

Comprueba si la configuración de seguridad de Amazon EMR tiene habilitado el cifrado en tránsito. La regla no cumple con las normas si está configurada. SecurityConfiguration. EncryptionConfiguration. EnableInTransitEncryption es falso.

Identificador: EMR_SECURITY_CONFIGURATION_ENCRYPTION_TRANSIT

Tipos de recursos: AWS::EMR::SecurityConfiguration

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

encrypted-volumes

Comprueba si los volúmenes de Amazon EBS adjuntos están cifrados y, de forma opcional, si están cifrados con una clave de KMS específica. La regla es NON_COMPLIANT si los volúmenes de EBS adjuntos no están cifrados o se han cifrado con una clave de KMS que no figura en los parámetros proporcionados.

Identificador: ENCRYPTED_VOLUMES

Tipos de recursos: AWS::EC2::Volume

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

kmsId (opcional), Tipo: cadena

ID o ARN de la clave KMS que se utiliza para cifrar el volumen.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

event-data-store-cmk-cifrado activado

Comprueba si los almacenes de datos de eventos de AWS Cloud Trail tienen habilitadas las claves AWS KMS administradas por el cliente. La regla es NON_COMPLIANT si un almacén de datos de eventos ha deshabilitado las claves de KMS administradas por el cliente. También puede especificar una lista de claves de KMS que la regla debe comprobar.

Identificador: EVENT_DATA_STORE_CMK_ENCRYPTION_ENABLED

Tipos de recursos: AWS::CloudTrail::EventDataStore

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

> Lista de nombres de recursos de Amazon (ARNs) de claves de AWS KMS separados por comas para que la regla los compruebe. Si se proporciona, la regla no cumple con las normas si un almacén de datos de eventos de AWS Cloud Trail no está cifrado con una de estas claves de KMS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

evidently-launch-description

Comprueba si los lanzamientos de Amazon CloudWatch Evidently tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: EVIDENTLY_LAUNCH_DESCRIPTION

Tipos de recursos: AWS::Evidently::Launch

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

evidently-launch-tagged

Comprueba si los lanzamientos de Amazon CloudWatch Evidentemente tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EVIDENTLY_LAUNCH_TAGGED

Tipos de recursos: AWS::Evidently::Launch

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

evidently-project-description

Comprueba si los proyectos de Amazon CloudWatch Evidently tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: EVIDENTLY_PROJECT_DESCRIPTION

Tipos de recursos: AWS::Evidently::Project

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

evidently-project-tagged

Comprueba si los proyectos de Amazon CloudWatch Evidently tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EVIDENTLY_PROJECT_TAGGED

Tipos de recursos: AWS::Evidently::Project

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

evidently-segment-description

Comprueba si los segmentos de Amazon CloudWatch Evidently tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: EVIDENTLY_SEGMENT_DESCRIPTION

Tipos de recursos: AWS::Evidently::Segment

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

evidently-segment-tagged

Comprueba si los segmentos de Amazon CloudWatch Evidently tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: EVIDENTLY_SEGMENT_TAGGED

Tipos de recursos: AWS::Evidently::Segment

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

fis-experiment-template-log-configuración-existe

Comprueba si las plantillas AWS de experimentos de la FIS tienen configurado el registro de experimentos. La regla no cumple con las normas si está configurada. LogConfiguration no existe.

Identificador: FIS_EXPERIMENT_TEMPLATE_LOG_CONFIGURATION_EXISTS

Tipos de recursos: AWS::FIS::ExperimentTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

fis-experiment-template-tagged

Comprueba si las plantillas AWS de experimentos del FIS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: FIS_EXPERIMENT_TEMPLATE_TAGGED

Tipos de recursos: AWS::FIS::ExperimentTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

fms-shield-resource-policy-comprobar

> **Note**
>
> Esta regla se encuentra actualmente en proceso de obsolescencia. No recomendamos utilizarla directamente.

Comprueba si los recursos que AWS Shield Avanzado puede proteger están protegidos por Shield Avanzado. La regla es NON_COMPLIANT si hay un recurso especificado que no está protegido.

Identificador: FMS_SHIELD_RESOURCE_POLICY_CHECK

Tipos de recursos: AWS::CloudFront::Distribution AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::WAFRegional::WebACL, AWS::EC2::EIP, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ShieldRegional::Protection, AWS::Shield::Protection

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

web ACLId, Tipo: cadena

Un identificador único para una ACL web.

resourceTypes, Tipo: cadena

Los tipos de recursos que especifique que la regla debe comprobar.

resourceTags (opcional), Tipo: cadena

Las etiquetas de recursos que especifique que la regla debe comprobar. Por ejemplo, { “tagKey1” : [“tagValue1”], “tagKey2” : [“tagValue2”, “tagValue3”] }.

excludeResourceTags (Opcional), Tipo: booleano

Si es True, la regla excluye los recursos especificados en resourceTags. Si es False, la regla incluye todos los recursos especificados en resourceTags.

fmsManagedToken (Opcional), Tipo: cadena

Un token generado por el AWS Firewall Manager al crear la regla en su cuenta. AWS Config ignora este parámetro al crear esta regla.

fmsRemediationEnabled (Opcional), Tipo: booleano

Si es verdadero, AWS Firewall Manager actualizará los recursos NON_COMPLIANT de acuerdo con la política de FMS. AWS Config ignora este parámetro al crear esta regla.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

fms-webacl-resource-policy-comprobar

> **Note**
>
> Esta regla se encuentra actualmente en proceso de obsolescencia. No recomendamos utilizarla directamente.

Comprueba si la ACL web está asociada a un Application Load Balancer, a una etapa de API Gateway o a distribuciones de Amazon CloudFront . Al AWS Firewall Manager crear esta regla, el propietario de la política de FMS la especifica `WebACLId` en la política de FMS y, si lo desea, puede habilitar la corrección.

Identificador: FMS_WEBACL_RESOURCE_POLICY_CHECK

Tipos de recursos: AWS::CloudFront::Distribution,,, AWS::ApiGateway::Stage AWS::ElasticLoadBalancingV2::LoadBalancer AWS::WAFRegional::WebACL

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

web ACLId, Tipo: cadena

La web ACLId de la web ACL.

resourceTags (opcional), Tipo: cadena

Las etiquetas de recursos (ApplicationLoadBalancer ApiGatewayStage y CloudFront las distribuciones) a las que debe estar asociada la regla. (por ejemplo, {«tagKey1": [" tagValue1"], «tagKey2": [" tagValue2", «tagValue3"]})

excludeResourceTags (Opcional), Tipo: booleano

Si es true, excluya los recursos que coincidan con resourceTags.

fmsManagedToken (Opcional), Tipo: cadena

Un token generado por el AWS Firewall Manager al crear la regla en la cuenta del cliente. AWS Config ignora este parámetro cuando el cliente crea esta regla.

fmsRemediationEnabled (Opcional), Tipo: booleano

Si es verdadero, AWS Firewall Manager actualizará los recursos no conformes de acuerdo con la política de FMS. AWS Config ignora este parámetro cuando el cliente crea esta regla.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

fms-webacl-rulegroup-association-comprobar

> **Note**
>
> Esta regla se encuentra actualmente en proceso de obsolescencia. No recomendamos utilizarla directamente.

Comprueba si los grupos de reglas se asocian a la ACL web con la prioridad correcta. La prioridad correcta se decide mediante la clasificación de los grupos de reglas en el parámetro ruleGroups. Cuando AWS Firewall Manager crea esta regla, asigna la prioridad más alta 0 seguido de 1, 2, etc. El propietario de la política de FMS especifica el rango `ruleGroups` en la política de FMS y tiene la opción de habilitar la corrección.

Identificador: FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

Tipos de recursos: AWS::WAF::WebACL, AWS::WAFRegional::WebACL

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

ruleGroups, Tipo: cadena

Lista de pares y separados por comas. RuleGroupIds WafOverrideAction (por ejemplo, ruleGroupId -1:NONE, 2:COUNT) ruleGroupId

fmsManagedToken (Opcional), Tipo: cadena

Un token generado por el AWS Firewall Manager al crear la regla en la cuenta del cliente. AWS Config ignora este parámetro cuando el cliente crea esta regla.

fmsRemediationEnabled (Opcional), Tipo: booleano

Si es verdadero, AWS Firewall Manager actualizará los recursos no conformes de acuerdo con la política de FMS. AWS Config ignora este parámetro cuando el cliente crea esta regla.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

frauddetector-entity-type-tagged

Comprueba si los tipos de entidad de Amazon Fraud Detector tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: FRAUDDETECTOR_ENTITY_TYPE_TAGGED

Tipos de recursos: AWS::FraudDetector::EntityType

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en el Este de EE. UU. (Ohio), Europa (Irlanda), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

frauddetector-label-tagged

Comprueba si las etiquetas de Amazon Fraud Detector tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: FRAUDDETECTOR_LABEL_TAGGED

Tipos de recursos: AWS::FraudDetector::Label

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en el Este de EE. UU. (Ohio), Europa (Irlanda), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

frauddetector-outcome-tagged

Comprueba si los resultados de Amazon Fraud Detector tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: FRAUDDETECTOR_OUTCOME_TAGGED

Tipos de recursos: AWS::FraudDetector::Outcome

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en el Este de EE. UU. (Ohio), Europa (Irlanda), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

frauddetector-variable-tagged

Comprueba si las variables de Amazon Fraud Detector tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: FRAUDDETECTOR_VARIABLE_TAGGED

Tipos de recursos: AWS::FraudDetector::Variable

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en el Este de EE. UU. (Ohio), Europa (Irlanda), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

fsx-last-backup-recovery-punto creado

Comprueba si se creó un punto de recuperación para Amazon FSx File Systems. La regla no es conforme si el Sistema de FSx Archivos de Amazon no tiene un punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::FSx::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de Amazon FSx File Systems para que la regla las compruebe, en formato JSON`{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID del sistema de FSx archivos de Amazon para comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

fsx-lustre-copy-tags-copias de seguridad

Comprueba si los sistemas de archivos Amazon FSx for Lustre están configurados para copiar etiquetas a las copias de seguridad. La regla es NON_COMPLIANT si los sistemas de archivos de Lustre no están configurados para copiar etiquetas en las copias de seguridad.

Identificador: FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

Tipos de recursos: AWS::FSx::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

fsx-meets-restore-time-objetivo

Comprueba si el tiempo de restauración de Amazon FSx File Systems cumple con la duración especificada. La regla es NON_COMPLIANT si LatestRestoreExecutionTimeMinutes la duración de un sistema de FSx archivos de Amazon es superior maxRestoreTime a minutos.

Identificador: FSX_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::FSx::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

maxRestoreTime, Tipo: int

Valor numérico del tiempo de ejecución de restauración máximo permitido.

resourceTags (opcional), Tipo: cadena

Etiquetas de Amazon FSx File Systems para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID del sistema de FSx archivos de Amazon para comprobar la regla.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

fsx-ontap-deployment-type-comprobar

Comprueba si los sistemas de archivos de Amazon FSx for NetApp ONTAP están configurados con determinados tipos de implementación. La regla es NON_COMPLIANT si los sistemas de archivos de Amazon FSx for NetApp ONTAP no están configurados con los tipos de despliegue que especifiques.

Identificador: FSX_ONTAP_DEPLOYMENT_TYPE_CHECK

Tipos de recursos: AWS::FSx::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

deploymentTypes, Tipo: CSV

Lista separada por comas de tipos de implementaciones que la regla debe comprobar.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

fsx-openzfs-copy-tags-habilitado

Comprueba si los sistemas de archivos Amazon FSx for OpenZFS están configurados para copiar etiquetas en copias de seguridad y volúmenes. La regla no cumple con los requisitos si los sistemas

de archivos OpenZFS no están configurados FSx para copiar etiquetas en copias de seguridad y volúmenes.

Identificador: FSX_OPENZFS_COPY_TAGS_ENABLED

Tipos de recursos: AWS::FSx::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

fsx-openzfs-deployment-type-comprobar

Comprueba si los sistemas de archivos Amazon FSx for OpenZFS están configurados con determinados tipos de implementación. La regla no es compatible si FSx los sistemas de archivos OpenZFS no están configurados con los tipos de implementación que especifique.

Identificador: FSX_OPENZFS_DEPLOYMENT_TYPE_CHECK

Tipos de recursos: AWS::FSx::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

deploymentTypes, Tipo: CSV

Lista separada por comas de tipos de implementaciones que la regla debe comprobar.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

fsx-resources-protected-by-plan de respaldo

Comprueba si Amazon FSx File Systems está protegido por un plan de copias de seguridad. La regla no cumple con los requisitos si el sistema de FSx archivos de Amazon no está cubierto por un plan de respaldo.

Identificador: FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::FSx::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de Amazon FSx File Systems para que la regla las compruebe, en formato JSON`{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID del sistema de FSx archivos de Amazon para comprobar la regla.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

fsx-windows-audit-log-configurado

Comprueba si los sistemas de archivos de Amazon FSx para Windows File Server tienen habilitada la auditoría de acceso a los archivos. La regla no es compatible si los sistemas de archivos del servidor FSx de archivos de Windows no tienen habilitada la auditoría de acceso a los archivos.

Identificador: FSX_WINDOWS_AUDIT_LOG_CONFIGURED

Tipos de recursos: AWS::FSx::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

fsx-windows-deployment-type-comprobar

Comprueba si los sistemas de archivos de Amazon FSx para WINDOWS están configurados con determinados tipos de despliegue. La regla no es compatible si los sistemas de archivos FSx de WINDOWS no están configurados con los tipos de implementación que especifique.

Identificador: FSX_WINDOWS_DEPLOYMENT_TYPE_CHECK

Tipos de recursos: AWS::FSx::FileSystem

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Europa (París), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

deploymentTypes, Tipo: CSV

Lista separada por comas de tipos de implementaciones que la regla debe comprobar.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

glb-listener-tagged

Comprueba si los oyentes del Equilibrador de carga de puerta de enlace tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: GLB_LISTENER_TAGGED

Tipos de recursos: AWS::ElasticLoadBalancingV2::Listener

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

glb-tagged

Comprueba si los Equilibradores de carga de puerta de enlace tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: GLB_TAGGED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

global-endpoint-event-replication-habilitado

Comprueba si la replicación de eventos está habilitada para los puntos finales EventBridge globales de Amazon. La regla es NON_COMPLIANT si la replicación de eventos no está habilitada.

Identificador: GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

Tipos de recursos: AWS::Events::Endpoint

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Osaka), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

glue-job-logging-enabled

Comprueba si un trabajo de AWS Glue tiene activado el registro. La regla no es conforme si un trabajo de AWS Glue no tiene habilitados CloudWatch los registros de Amazon.

Identificador: GLUE_JOB_LOGGING_ENABLED

Tipos de recursos: AWS::Glue::Job

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

glue-ml-transform-encrypted-en reposo

Comprueba si una transformación de AWS Glue ML tiene activado el cifrado en reposo. La regla NO ES COMPATIBLE si `` se establece en MLUser DataEncryptionMode `DISABLED`.

Identificador: GLUE_ML_TRANSFORM_ENCRYPTED_AT_REST

Tipos de recursos: AWS::Glue::MLTransform

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

glue-ml-transform-tagged

Comprueba si las transformaciones de aprendizaje automático de AWS Glue tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: GLUE_ML_TRANSFORM_TAGGED

Tipos de recursos: AWS::Glue::MLTransform

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

glue-spark-job-supported-versión

Comprueba si un trabajo de AWS Glue Spark se está ejecutando en la versión de AWS Glue mínima admitida especificada. La regla no es conforme si el trabajo de AWS Glue Spark no se ejecuta en la versión de AWS Glue mínima admitida que especifiques.

Identificador: GLUE_SPARK_JOB_SUPPORTED_VERSION

Tipos de recursos: AWS::Glue::Job

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

minimumSupportedGlueVersión, Tipo: cadena

Debe especificar el valor de cadena de caracteres de la versión mínima de AWS Glue admitida para que la regla lo compruebe.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

servicio de guardia -ec2- protection-runtime-enabled

Comprueba si el monitoreo de tiempo de ejecución de ECS con administración automática de agentes está habilitado para Amazon GuardDuty Detector. La regla es NON_COMPLIANT si la característica no está habilitada para la cuenta o al menos una cuenta de miembro de la organización.

Identificador: EC2 GUARDDUTY_ _PROTECTION_RUNTIME_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guardduty-ecs-protection-runtime-habilitado

Comprueba si el monitoreo de tiempo de ejecución de ECS con administración automática de agentes está habilitado para Amazon GuardDuty Detector. La regla es NON_COMPLIANT si la característica no está habilitada para la cuenta o al menos una cuenta de miembro de la organización.

Identificador: GUARDDUTY_ECS_PROTECTION_RUNTIME_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guardduty-eks-protection-audit-habilitado

Comprueba si la monitorización de registros de auditoría para Amazon Elastic Kubernetes Service (Amazon EKS) está habilitada para un detector de GuardDuty Amazon en su cuenta. La regla es

NON_COMPLIANT si la característica de supervisión de registros de auditoría de EKS no está habilitada para la cuenta.

Identificador: GUARDDUTY_EKS_PROTECTION_AUDIT_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

guardduty-eks-protection-runtime-habilitado

Comprueba si Amazon EKS Runtime Monitoring con administración automatizada de agentes está habilitada para el GuardDuty detector en su cuenta. La regla no cumple con los requisitos si el monitoreo de tiempo de ejecución de EKS con administración automática de agentes no GuardDuty está activado en su cuenta.

Identificador: GUARDDUTY_EKS_PROTECTION_RUNTIME_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guardduty-enabled-centralized

Comprueba si Amazon GuardDuty está activado en tu AWS cuenta y AWS región. Si proporciona una AWS cuenta para la centralización, la regla evalúa los GuardDuty resultados en la cuenta centralizada. La regla cumple con las normas cuando GuardDuty está habilitada.

Identificador: GUARDDUTY_ENABLED_CENTRALIZED

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

CentralMonitoringAccount (Opcional), Tipo: cadena

> Lista de AWS cuentas separadas por comas (12 dígitos) en las que se permite GuardDuty centralizar los resultados de Amazon.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guardduty-lambda-protection-enabled

Comprueba si la Protección Lambda está habilitada para un GuardDuty detector de Amazon en su cuenta. La regla no cumple con las normas si la función Lambda Protection de Amazon no GuardDuty está habilitada para su cuenta.

Identificador: GUARDDUTY_LAMBDA_PROTECTION_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guardduty-malware-protection-enabled

Comprueba si la protección contra malware está habilitada para un GuardDuty detector de Amazon en tu cuenta. La regla no es conforme si la función de protección contra malware de Amazon no GuardDuty está habilitada para tu cuenta.

Identificador: GUARDDUTY_MALWARE_PROTECTION_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guardduty-non-archived-findings

Comprueba si Amazon GuardDuty tiene hallazgos que no están archivados. La regla no es conforme si GuardDuty tiene el parámetro/no archivado. low/medium/high severity findings older than the specified number in the daysLowSev/daysMediumSev `daysHighSev`

Identifier (Identificador): GUARDDUTY_NON_ARCHIVED_FINDINGS

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

daysLowSev (Opcional), Tipo: int, Valor predeterminado: 30

> El número de días que se permite que los hallazgos de GuardDuty baja gravedad de Amazon permanezcan sin archivar. El valor predeterminado es 30 días.

daysMediumSev (Opcional), Tipo: int, Valor predeterminado: 7

> El número de días que se permite que las conclusiones de gravedad GuardDuty media de Amazon permanezcan sin archivar. El valor predeterminado es de 7 días.

daysHighSev (Opcional), Tipo: int, Valor predeterminado: 1

> El número de días que se permite que los hallazgos de GuardDuty alta gravedad de Amazon permanezcan sin archivar. El valor predeterminado es 1.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

guardduty-rds-protection-enabled

Comprueba si la protección de Amazon Relational Database Service (Amazon RDS) está habilitada para un detector de GuardDuty Amazon en su cuenta. La regla no es conforme si la función de protección Amazon RDS de Amazon no GuardDuty está habilitada para tu cuenta.

Identificador: GUARDDUTY_RDS_PROTECTION_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guardduty-runtime-monitoring-enabled

Comprueba si la monitorización del tiempo de ejecución está habilitada para Amazon GuardDuty Detector en tu cuenta u organización. La regla NO CUMPLE CON LOS REQUISITOS si Runtime Monitoring in no GuardDuty está activado en su cuenta o en la de al menos una cuenta de un miembro de su organización.

Identificador: GUARDDUTY_RUNTIME_MONITORING_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guardduty-s3-protection-enabled

Comprueba si la protección S3 está habilitada para un Amazon GuardDuty Detector en tu cuenta. La regla no cumple con las normas si la función de protección S3 de Amazon no GuardDuty está habilitada para tu cuenta.

Identificador: GUARDDUTY_S3_PROTECTION_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-customer-policy-blocked-kms-acciones

Comprueba si las políticas gestionadas de AWS Identity and Access Management (IAM) que ha creado no permiten bloquear acciones de KMS en todos los AWS recursos clave de KMS. La regla no cumple con los requisitos si la política de IAM gestionada permite realizar cualquier acción de bloqueo en todas las claves de AWS KMS.

> **Note**
>
> Para que se considere no pública, una política de SQS debe conceder acceso solo a valores fijos. Esto significa valores que no contienen un comodín ni el siguiente elemento de política de IAM: Variables.

Identificador: IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

Tipos de recursos: AWS::IAM::Policy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

blockedActionsPatterns, Tipo: CSV

Lista separada por comas de patrones de acción de KMS bloqueados bloqueados que debe comprobar la regla. La regla es NON_COMPLIANT si las políticas administradas por el cliente de IAM otorgan acceso comodín a todos los recursos para las acciones que especifique.

excludePermissionBoundaryPolítica (opcional), Tipo: booleano

Indicador booleano para excluir la evaluación de las políticas de IAM utilizadas como límites de permisos. Si se establece en true, la regla no incluirá los límites de permisos en la evaluación. De lo contrario, todas las políticas de IAM incluidas en el ámbito de aplicación se evaluarán cuando el valor se establezca en false. El valor predeterminado es false.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-external-access-analyzer-habilitado

Comprueba si hay un Analizador de acceso de IAM para acceso externo activado en la cuenta por región. La regla es NON_COMPLIANT si no hay analizadores para el acceso externo en la región o si el atributo “status” no se ha definido como ACTIVE.

Identificador: IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iam-group-has-users-comprobar

Comprueba si los grupos de IAM tienen al menos un usuario de IAM.

Identificador: IAM_GROUP_HAS_USERS_CHECK

Tipos de recursos: AWS::IAM::Group

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico

(Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iam-inline-policy-blocked-kms-acciones

Comprueba si las políticas integradas asociadas a sus usuarios, roles y grupos de IAM no permiten el bloqueo de acciones en todas las claves de KMS. AWS La regla no cumple con los requisitos si se permite alguna acción de bloqueo en todas las claves de AWS KMS de una política en línea.

Identificador: IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

Tipos de recursos:,, AWS::IAM::Group AWS::IAM::Role AWS::IAM::User

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

blockedActionsPatterns, Tipo: CSV

Lista separada por comas de patrones de acción de KMS bloqueados, por ejemplo, *, Decrypt, kms: *. kms: kms: ReEncrypt

excludeRoleByManagementAccount (Opcional), Tipo: booleano

Excluya un rol si solo lo puede asumir la cuenta de administración de la organización.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iam-no-inline-policy-comprobar

Comprueba si la característica de política integrada no está en uso. La regla no es compatible si un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM tiene alguna política en línea.

Identificador: IAM_NO_INLINE_POLICY_CHECK

AWS::IAM::Group AWS::IAM::RoleTipos de recursos:,, AWS::IAM::User

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), EE. UU. Oeste (Norte de California), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iam-oidc-provider-tagged

Comprueba si los proveedores de AWS IAM OIDC tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IAM_OIDC_PROVIDER_TAGGED

Tipos de recursos: AWS::IAM::OIDCProvider

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iam-password-policy

Comprueba si la política de contraseñas de la cuenta para los usuarios de AWS Identity and Access Management (IAM) cumple los requisitos especificados que se indican en los parámetros. La regla es NON_COMPLIANT si la política de contraseñas de la cuenta no cumple con los requisitos especificados.

> **Important**
>
> Los valores `true` y `false` de los parámetros de la regla distinguen entre mayúsculas y minúsculas. Si `true` no está en minúsculas, se tratará como `false`..

> **Note**
>
> Resultado de la evaluación en la política de contraseñas de IAM predeterminada
> Esta regla se marca como NON_COMPLIANT cuando se utiliza la política de contraseñas de IAM predeterminada.
> Reglas administradas y tipos de recursos de IAM globales
> Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo

se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.
Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.
A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Identificador: IAM_PASSWORD_POLICY

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

RequireUppercaseCharacters (Opcional), Tipo: booleano, Predeterminado: true

Requiere que al menos haya un carácter en mayúscula en la contraseña.

RequireLowercaseCharacters (Opcional), Tipo: booleano, Predeterminado: true

Requiere que al menos haya un carácter en minúscula en la contraseña.

RequireSymbols (Opcional), Tipo: booleano, Predeterminado: true

Requiere que al menos haya un símbolo en la contraseña.

RequireNumbers (Opcional), Tipo: booleano, Predeterminado: true

Requiere que al menos haya un número en la contraseña.

MinimumPasswordLength (Opcional), Tipo: int, Valor predeterminado: 14

Longitud mínima de la contraseña.

PasswordReusePrevention (Opcional), Tipo: int, Valor predeterminado: 24

Número de contraseñas antes de que se permita reutilizarlas.

MaxPasswordAge (Opcional), Tipo: int, Valor predeterminado: 90

Número de días antes de la contraseña venza.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-policy-blacklisted-check

Comprueba en cada recurso de AWS Identity and Access Management (IAM) (IAM) si hay una política denominada Amazon Resource Name (ARN) en el parámetro de entrada asociada al recurso de IAM. La regla es NON_COMPLIANT si el ARN de la política está asociado al recurso de IAM.

Identificador: IAM_POLICY_BLACKLISTED_CHECK

Tipos de recursos:,, AWS::IAM::User AWS::IAM::Group AWS::IAM::Role

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

policyArns, Tipo: CSV, Predeterminado: arn:aws:iam: :aws:policy/ AdministratorAccess

Lista separada por comas de los ARN de las políticas de IAM que no se deben asociar a ninguna entidad de IAM.

exceptionList (opcional), Tipo: CSV

Lista separada por comas de tipos de recursos y lista de pares de nombres de recursos. Por ejemplo, los usuarios: [user1;user2], grupos: [group1;group2], funciones: [role1;role2;role3].

> **Note**
>
> Para la lista de excepciones, especifique el nombre del recurso, no el ARN completo. No válido: `arn:aws:iam::444455556666:role/Admin`. Válido: `Admin`.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-policy-in-use

Comprueba si el ARN de la política de IAM está asociado a un usuario de IAM o a un grupo con uno o varios usuarios de IAM o un rol de IAM con una o varias entidades de confianza.

> **Note**
>
> Reglas administradas y tipos de recursos de IAM globales
> Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.
> Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.
> A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Identificador: IAM_POLICY_IN_USE

Tipos de recursos: AWS::IAM::Policy

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

policyARN, Tipo: cadena

Un ARN de política de IAM que debe comprobarse.

policyUsageType (Opcional), Tipo: cadena

Especifica si espera que la política se adjunte a un usuario, grupo o rol de IAM. Los valores válidos son IAM_USER, IAM_GROUP, IAM_ROLE o ANY. El valor predeterminado es ANY (CUALQUIERA).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-policy-no-statements-with-admin-access

Comprueba si las políticas de AWS Identity and Access Management (IAM) que cree tienen instrucciones de permiso que conceden permisos a todas las acciones de todos los recursos. La regla es NON_COMPLIANT (NO CONFORME) si alguna instrucción de la política de IAM administrada por el cliente contiene "Effect": "Allow" con "Action": "*" sobre "Resource": "*".

> **Note**
>
> Esta regla solo evalúa las políticas administradas por el cliente. Esta regla NO evalúa las políticas integradas ni las políticas AWS administradas. Para obtener más información sobre la diferencia, consulte Políticas administradas y políticas insertadas en la Guía del usuario de IAM.

La siguiente política es NON_COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

La siguiente política es COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

Identificador: IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

Tipos de recursos: AWS::IAM::Policy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

excludePermissionBoundaryPolítica (opcional), Tipo: booleano

> Indicador booleano para excluir la evaluación de las políticas de IAM utilizadas como límites de permisos. Si se establece en true, la regla no incluirá los límites de permisos en la evaluación. De lo contrario, todas las políticas de IAM incluidas en el ámbito de aplicación se evaluarán cuando el valor se establezca en false. El valor predeterminado es false.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-policy-no-statements-with-full-access

Comprueba si las políticas de AWS Identity and Access Management (IAM) que cree conceden permisos para todas las acciones de los recursos individuales. AWS La regla no cumple con los requisitos si alguna política de IAM gestionada por el cliente permite el acceso total a al menos un servicio. AWS

Contexto: con base en el principio del privilegio mínimo, es recomendable limitar las acciones permitidas en las políticas de IAM al conceder permisos a los servicios de AWS . Este método ayuda a garantizar que solo se concedan los permisos necesarios especificando las acciones necesarias exactas, lo que evita el uso sin restricciones de comodines para un servicio, como `ec2:*`.

En algunos casos, es posible que desee permitir varias acciones con un prefijo similar, como y. DescribeFlowLogsDescribeAvailabilityZones En estos casos, puede añadir un comodín con sufijo al prefijo común (por ejemplo, `ec2:Describe*`). Agrupar las acciones relacionadas puede contribuir a no alcanzar los límites de tamaño de las políticas de IAM.

Esta regla devolverá COMPLIANT si utiliza acciones con prefijos y con un comodín como sufijo (como `ec2:Describe*`). Esta regla solo devolverá NON_COMPLIANT si utiliza comodines sin restricciones (como, `ec2:*`).

> **Note**
>
> Esta regla solo evalúa las políticas administradas por el cliente. Esta regla NO evalúa las políticas integradas ni las políticas AWS gestionadas. Para obtener más información sobre la diferencia, consulte Políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Identificador: IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

Tipos de recursos: AWS::IAM::Policy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

excludePermissionBoundaryPolítica (opcional), Tipo: booleano

> Indicador booleano para excluir la evaluación de las políticas de IAM utilizadas como límites de permisos. Si se establece en true, la regla no incluirá los límites de permisos en la evaluación. De lo contrario, todas las políticas de IAM incluidas en el ámbito de aplicación se evaluarán cuando el valor se establezca en false. El valor predeterminado es false.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iam-role-managed-policy-comprobar

Comprueba si todas las políticas gestionadas especificadas en la lista de políticas gestionadas están asociadas a la función AWS Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si el rol de IAM no está asociado a ninguna política administrada.

Identificador: IAM_ROLE_MANAGED_POLICY_CHECK

Tipos de recursos: AWS::IAM::Role

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

managedPolicyArns, Tipo: CSV

Lista separada por comas de nombres de recursos de Amazon para políticas AWS gestionadas ()ARNs. Para obtener más información, consulte Nombres de recursos de Amazon (ARNs) y políticas AWS administradas en la Guía del usuario de IAM.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-root-access-key-comprobar

Comprueba si la clave de acceso del usuario raíz está disponible. La regla es COMPLIANT si la clave de acceso del usuario no existe. De lo contrario, es NON_COMPLIANT.

> **Note**
>
> Reglas administradas y tipos de recursos de IAM globales
> Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.
> Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.
> A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Identificador: IAM_ROOT_ACCESS_KEY_CHECK

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-saml-provider-tagged

Comprueba si los proveedores de SAML de AWS IAM tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IAM_SAML_PROVIDER_TAGGED

Tipos de recursos: AWS::IAM::SAMLProvider

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-server-certificate-expiration-comprobar

Comprueba si los certificados de SSL/TLS servidor de AWS IAM almacenados en IAM han caducado. La regla es NON_COMPLIANT si un certificado de servidor de IAM ha caducado.

Identificador: IAM_SERVER_CERTIFICATE_EXPIRATION_CHECK

Tipos de recursos: AWS::IAM::ServerCertificate

Tipo de disparador: periódico

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-server-certificate-tagged

Comprueba si los certificados del servidor de AWS IAM tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IAM_SERVER_CERTIFICATE_TAGGED

Tipos de recursos: AWS::IAM::ServerCertificate

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-user-group-membership-comprobar

Comprueba si los usuarios de IAM son miembros de al menos un grupo de IAM.

Identificador: IAM_USER_GROUP_MEMBERSHIP_CHECK

Tipos de recursos: AWS::IAM::User

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

groupNames (opcional), Tipo: CSV

Lista separada por comas de grupos de IAM a los que deben pertenecer los usuarios de IAM.

> **Note**
>
> Esta regla no admite nombres de grupo con comas.

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-user-mfa-enabled

Comprueba si los usuarios de AWS Identity and Access Management (IAM) tienen habilitada la autenticación multifactor (MFA). La regla es NON_COMPLIANT si la MFA no está habilitada para al menos un usuario de IAM.

> **Note**
>
> Reglas administradas y tipos de recursos de IAM globales
> Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.
> Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.
> A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Identificador: IAM_USER_MFA_ENABLED

Tipos de recursos: AWS::IAM::User

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico

(Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-user-no-policies-comprobar

Comprueba si ninguno de sus usuarios de AWS Identity and Access Management (IAM) tiene políticas adjuntas. Los usuarios de IAM deben heredar los permisos de los grupos o roles de IAM. La regla es NON_COMPLIANT si hay al menos una política asociada al usuario de IAM.

Identificador: IAM_USER_NO_POLICIES_CHECK

Tipos de recursos: AWS::IAM::User

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iam-user-unused-credentials-comprobar

Comprueba si sus usuarios AWS Identity and Access Management (de IAM) tienen contraseñas o claves de acceso activas que no se hayan utilizado en el número de días especificado que usted

proporcionó. La regla es NON_COMPLIANT si hay cuentas inactivas que no se han utilizado recientemente.

> **Note**
>
> Plazo de reevaluación
> Volver a evaluar esta regla en un plazo de 4 horas tras la primera evaluación no tendrá ningún efecto en los resultados.
> Reglas administradas y tipos de recursos de IAM globales
> Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.
> Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.
> A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Identificador: IAM_USER_UNUSED_CREDENTIALS_CHECK

Tipos de recursos: AWS::IAM::User

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

maxCredentialUsageEdad, Tipo: int, Valor predeterminado: 90

Número máximo de días durante los que no se puede usar una credencial. El valor predeterminado es 90 días.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

restricted-ssh

> **Important**
>
> Para esta regla, el identificador de la regla (INCOMING_SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferentes.

Comprueba si el tráfico SSH entrante de los grupos de seguridad es accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario, es NON_COMPLIANT.

Identificador: INCOMING_SSH_DISABLED

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de desencadenador: cambios de configuración y periódicos

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

inspector-ec2-scan-enabled

Comprueba si el EC2 escaneo de Amazon Inspector V2 está activado en su entorno de una o varias cuentas para detectar posibles vulnerabilidades y problemas de acceso a la red en sus instancias. EC2 La regla no cumple con los requisitos si EC2 el escaneo no está activado.

Identificador: INSPECTOR_ _SCAN_ENABLED EC2

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

inspector-ecr-scan-enabled

Comprueba si el análisis de ECR de Amazon Inspector V2 está activado en el entorno, de una o varias cuentas, a fin de detectar posibles vulnerabilidades en las imágenes de contenedor. La regla es NON_COMPLIANT si el análisis de ECR no está activado.

Identificador: INSPECTOR_ECR_SCAN_ENABLED

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico

(Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

inspector-lambda-code-scan-habilitado

Comprueba si el análisis de código de Lambda con Amazon Inspector V2 está activado en el entorno, de una o varias cuentas, a fin de detectar posibles vulnerabilidades de código. La regla es NON_COMPLIANT si el análisis de código de Lambda no está activado.

Identificador: INSPECTOR_LAMBDA_CODE_SCAN_ENABLED

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

inspector-lambda-standard-scan-habilitado

Comprueba si el análisis estándar de Lambda con Amazon Inspector V2 está activado en el entorno de una o varias cuentas, a fin de detectar posibles vulnerabilidades de software. La regla es NON_COMPLIANT si el análisis estándar de Lambda no está activado.

Identificador: INSPECTOR_LAMBDA_STANDARD_SCAN_ENABLED

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ec-2 instances-in-vpc

> **Important**
>
> Para esta regla, el identificador de la regla (INSTANCES_IN_VPC) y el nombre de la regla (ec2-) son diferentes. instances-in-vpc

Comprueba si EC2 las instancias pertenecen a una nube privada virtual (VPC). Si lo prefiere, puede especificar el ID de VPC para asociarlo a sus instancias.

Identificador: INSTANCES_IN_VPC

Tipos de recursos: AWS::EC2::Instance

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

vpcId (opcional), Tipo: cadena

ID de VPC que contiene estas EC2 instancias.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

internet-gateway-authorized-vpc-solo

Comprueba si las puertas de enlace de Internet están conectadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

Identifier (Identificador): INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

Tipos de recursos: AWS::EC2::InternetGateway

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

AuthorizedVpcIds (Opcional), Tipo: CSV

Lista separada por comas de la IDs VPC autorizada y adjunta. IGWs Si no se proporciona el parámetro, todos los archivos adjuntos no IGWs serán conformes.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iotdevicedefender-custom-metric-tagged

AWS Las métricas personalizadas de IoT Device Defender tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTDEVICEDEFENDER_CUSTOM_METRIC_TAGGED

Tipos de recursos: AWS::IoT::CustomMetric

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Medio Oriente (Baréin), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Medio Oriente (EAU), Europa (Fráncfort), Asia-Pacífico (Hong Kong), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iotevents-alarm-model-tagged

Comprueba si los modelos de alarma de AWS IoT Events tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTEVENTS_ALARM_MODEL_TAGGED

Tipos de recursos: AWS::IoTEvents::AlarmModel

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iotevents-detector-model-tagged

Comprueba si los modelos de detectores de AWS IoT Events tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTEVENTS_DETECTOR_MODEL_TAGGED

Tipos de recursos: AWS::IoTEvents::DetectorModel

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico

(Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iotevents-input-tagged

Comprueba si AWS las entradas de IoT Events tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTEVENTS_INPUT_TAGGED

Tipos de recursos: AWS::IoTEvents::Input

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iotsitewise-asset-model-tagged

Comprueba si los modelos SiteWise de activos de AWS IoT tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTSITEWISE_ASSET_MODEL_TAGGED

Tipos de recursos: AWS::IoTSiteWise::AssetModel

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iotsitewise-dashboard-tagged

Comprueba si los SiteWise paneles de AWS IoT tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTSITEWISE_DASHBOARD_TAGGED

Tipos de recursos: AWS::IoTSiteWise::Dashboard

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iotsitewise-gateway-tagged

Comprueba si AWS las SiteWise pasarelas de IoT tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTSITEWISE_GATEWAY_TAGGED

Tipos de recursos: AWS::IoTSiteWise::Gateway

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iotsitewise-portal-tagged

Comprueba si los SiteWise portales de AWS IoT tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTSITEWISE_PORTAL_TAGGED

Tipos de recursos: AWS::IoTSiteWise::Portal

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iotsitewise-project-tagged

Comprueba si los SiteWise proyectos de AWS IoT tienen etiquetas. También puede especificar claves de etiqueta para la regla. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTSITEWISE_PROJECT_TAGGED

Tipos de recursos: AWS::IoTSiteWise::Project

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iottwinmaker-component-type-tagged

Comprueba si los tipos de TwinMaker componentes de AWS IoT tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTTWINMAKER_COMPONENT_TYPE_TAGGED

Tipos de recursos: AWS::IoTTwinMaker::ComponentType

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iottwinmaker-entity-tagged

Comprueba si TwinMaker las entidades de AWS IoT tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTTWINMAKER_ENTITY_TAGGED

Tipos de recursos: AWS::IoTTwinMaker::Entity

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iottwinmaker-scene-tagged

Comprueba si AWS las TwinMaker escenas de IoT tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTTWINMAKER_SCENE_TAGGED

Tipos de recursos: AWS::IoTTwinMaker::Scene

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iottwinmaker-sync-job-tagged

Comprueba si los trabajos de TwinMaker sincronización de AWS IoT tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTTWINMAKER_SYNC_JOB_TAGGED

Tipos de recursos: AWS::IoTTwinMaker::SyncJob

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iottwinmaker-workspace-tagged

Comprueba si los TwinMaker espacios de trabajo de AWS IoT tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTTWINMAKER_WORKSPACE_TAGGED

Tipos de recursos: AWS::IoTTwinMaker::Workspace

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iotwireless-fuota-task-tagged

Comprueba si AWS las tareas FUOTA de IoT Wireless tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTWIRELESS_FUOTA_TASK_TAGGED

Tipos de recursos: AWS::IoTWireless::FuotaTask

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iotwireless-multicast-group-tagged

Comprueba si los grupos de multidifusión de AWS IoT Wireless tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTWIRELESS_MULTICAST_GROUP_TAGGED

Tipos de recursos: AWS::IoTWireless::MulticastGroup

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iotwireless-service-profile-tagged

Comprueba si los perfiles del servicio AWS IoT Wireless tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOTWIRELESS_SERVICE_PROFILE_TAGGED

Tipos de recursos: AWS::IoTWireless::ServiceProfile

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón) y Asia-Pacífico (Sídney)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iot-authorizer-token-signing-habilitado

Comprueba si un autorizador de AWS IoT Core no ha desactivado los requisitos de firma para validar la firma del token en una solicitud de autorización. La regla NO CUMPLE CON LOS REQUISITOS si el autorizador tiene una configuración. SigningDisabled establecido en True.

Identificador: IOT_AUTHORIZER_TOKEN_SIGNING_ENABLED

Tipos de recursos: AWS::IoT::Authorizer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Región Oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iot-job-template-tagged

Comprueba si los recursos de plantillas de trabajo de AWS IoT tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOT_JOB_TEMPLATE_TAGGED

Tipos de recursos: AWS::IoT::JobTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Región Oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iot-provisioning-template-description

Comprueba si AWS las plantillas de aprovisionamiento de IoT tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: IOT_PROVISIONING_TEMPLATE_DESCRIPTION

Tipos de recursos: AWS::IoT::ProvisioningTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Región Oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iot-provisioning-template-jitp

Comprueba si AWS las plantillas de aprovisionamiento de IoT utilizan el just-in-time aprovisionamiento (JITP). La regla no cumple con las normas si está configurada. TemplateType no es «JITP».

Identificador: IOT_PROVISIONING_TEMPLATE_JITP

Tipos de recursos: AWS::IoT::ProvisioningTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Región Oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

iot-provisioning-template-tagged

Comprueba si AWS las plantillas de aprovisionamiento de IoT tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de

etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOT_PROVISIONING_TEMPLATE_TAGGED

Tipos de recursos: AWS::IoT::ProvisioningTemplate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Región Oeste (Calgary), Europa (España), China (Ningxia), Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

iot-scheduled-audit-tagged

Comprueba si AWS las auditorías programadas de IoT tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IOT_SCHEDULED_AUDIT_TAGGED

Tipos de recursos: AWS::IoT::ScheduledAudit

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Medio Oriente (Baréin), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Medio Oriente (EAU), Europa (Fráncfort), Asia-Pacífico (Hong Kong), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ivs-channel-playback-authorization-habilitado

Comprueba si los canales Amazon IVS tienen habilitada la autorización de reproducción. La regla es NON_COMPLIANT si configuration.Authorized es False.

Identificador: IVS_CHANNEL_PLAYBACK_AUTHORIZATION_ENABLED

Tipos de recursos: AWS::IVS::Channel

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ivs-channel-tagged

Comprueba si los canales de Amazon IVS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IVS_CHANNEL_TAGGED

Tipos de recursos: AWS::IVS::Channel

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ivs-playback-key-pair-etiquetado

Comprueba si los pares de claves de reproducción de Amazon IVS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de

etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IVS_PLAYBACK_KEY_PAIR_TAGGED

Tipos de recursos: AWS::IVS::PlaybackKeyPair

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ivs-recording-configuration-tagged

Comprueba si las configuraciones de registro de Amazon IVS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: IVS_RECORDING_CONFIGURATION_TAGGED

Tipos de recursos: AWS::IVS::RecordingConfiguration

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

kinesis-firehose-delivery-stream-encriptado

Comprueba si los flujos de entrega de Amazon Kinesis Data Firehose están cifrados en reposo con el cifrado del servidor. La regla es NON_COMPLIANT si hay un flujo de entrega de Kinesis Data Firehose que no se cifra en reposo con el cifrado del servidor.

Identificador: KINESIS_FIREHOSE_DELIVERY_STREAM_ENCRYPTED

Tipos de recursos: AWS::KinesisFirehose::DeliveryStream

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

> Lista separada por comas de los ARN de claves de KMS aprobados para el uso de Kinesis Firehose.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

kinesis-stream-backup-retention-comprobar

Comprueba si hay un Amazon Kinesis Data Stream con el período de retención de registro de datos establecido en un número específico de horas. La regla no cumple con los requisitos si la propiedad `RetentionPeriodHours` se establece en un valor inferior al valor especificado por el parámetro.

Identificador: KINESIS_STREAM_BACKUP_RETENTION_CHECK

Tipos de recursos: AWS::Kinesis::Stream

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

minimumBackupRetentionPeriodo (opcional), Tipo: cadena

> Se deben conservar los registros de datos durante un número mínimo de horas. Los valores válidos van de 24 a 8760 y el valor predeterminado es 168.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

kinesis-stream-encrypted

Comprueba si los flujos de Amazon Kinesis están cifrados en reposo con el cifrado del servidor. La regla no es conforme para una transmisión de Kinesis si 'StreamEncryption' no está presente.

Contexto: el cifrado del lado del servidor es una función de Amazon Kinesis Data Streams que cifra automáticamente los datos antes de que estén en reposo mediante una clave de KMS. AWS Los datos se cifran antes de escribirlos en la capa de almacenamiento del flujo de Kinesis y se descifran

después de recuperarlos del almacenamiento. Como resultado, los datos se cifran en reposo en el servicio de Kinesis Data Streams. Esto le permite cumplir requisitos normativos y mejorar la seguridad de sus datos. Para obtener más información, consulte Protección de datos en Amazon Kinesis Data Streams.

Identificador: KINESIS_STREAM_ENCRYPTED

Tipos de recursos: AWS::Kinesis::Stream

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

kinesis-video-stream-minimum-retención de datos

Comprueba si un Amazon Kinesis Video Stream está configurado con un valor mayor o igual que retención de datos mínima especificada. La regla no es compatible si DataRetentionInHours es inferior al valor especificado en el parámetro de regla obligatorio.

Identificador: KINESIS_VIDEO_STREAM_MINIMUM_DATA_RETENTION

Tipos de recursos: AWS::KinesisVideo::Stream

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Asia-Pacífico (Hong Kong), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney), Canadá (centro) y Canadá (centro)

Parámetros:

minDataRetentionInHours, Tipo: int

La retención de datos mínima en horas de la Amazon Kinesis Video Stream para que se compruebe la regla. La regla es NON_COMPLIANT si la retención de datos en horas es inferior al valor especificado en este parámetro. Los valores válidos van de 0 a 87600.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

kms-cmk-not-scheduled-para su eliminación

Comprueba si las AWS claves del Servicio de administración de claves (AWS KMS) no están programadas para su eliminación en AWS KMS. La regla es NON_COMPLIANT si las claves de KMS están programadas para la eliminación.

Identifier (Identificador): KMS_CMK_NOT_SCHEDULED_FOR_DELETION

Tipos de recursos: AWS::KMS::Key

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Europa (Milán) y Asia Pacífico (Taipéi)

Parámetros:

kmsKeyIds (Opcional), Tipo: cadena

(Opcional) IDs No se debe programar la eliminación de una lista separada por comas de claves específicas administradas por el cliente. Si no especifica ninguna clave, la regla comprueba todas las claves.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

kms-key-policy-no-acceso público

Comprueba si la política de claves de AWS KMS permite el acceso público. La regla es NON_COMPLIANT si la política de claves de KMS permite el acceso público a la clave de KMS.

> **Note**
>
> Para que se considere no pública, una política de clave de KMS debe conceder acceso solo a valores fijos. Esto significa valores que no contienen un comodín ni el siguiente elemento de política de IAM: Variables.

Identificador: KMS_KEY_POLICY_NO_PUBLIC_ACCESS

Tipos de recursos: AWS::KMS::Key

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

kms-key-tagged

Comprueba si las AWS claves del Servicio de administración de claves (KMS) tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: KMS_KEY_TAGGED

Tipos de recursos: AWS::KMS::Key

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

lambda-concurrency-check

Comprueba si la función de Lambda está configurada con el límite de ejecución simultánea de nivel de función. La regla es NON_COMPLIANT si la función de Lambda no está configurada con el límite de ejecución simultánea de nivel de función.

Identificador: LAMBDA_CONCURRENCY_CHECK

Tipos de recursos: AWS::Lambda::Function

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

ConcurrencyLimitHigh (Opcional), Tipo: cadena

> Límite máximo de ejecución de simultaneidad

ConcurrencyLimitLow (Opcional), Tipo: cadena

Límite mínimo de ejecución de simultaneidad

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

lambda-dlq-check

Comprueba si una función AWS Lambda está configurada con una cola de letra muerta. La regla es NON_COMPLIANT si la función de Lambda no está configurada con una cola de mensajes fallidos.

Identificador: LAMBDA_DLQ_CHECK

Tipos de recursos: AWS::Lambda::Function

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EEUU-Este), AWS GovCloud (EEUU-Oeste) y China (Ningxia)

Parámetros:

dlqArns (opcional), Tipo: CSV

Lista separada por comas de Amazon SQS y Amazon ARNs SNS que deben configurarse como destino de cola de letras muertas de la función Lambda

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

lambda-function-description

Comprueba si las funciones AWS Lambda tienen una descripción. La regla es NON_COMPLIANT si configuration.description no existe o es una cadena vacía.

Identificador: LAMBDA_FUNCTION_DESCRIPTION

Tipos de recursos: AWS::Lambda::Function

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), AWS GovCloud (EEUU-Este), AWS GovCloud (EEUU-Oeste) y China (Ningxia) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

lambda-function-public-access-prohibido

Comprueba si la política de AWS Lambda funciones adjunta al recurso de Lambda prohíbe el acceso público. Si la política de la función de Lambda permite el acceso público, es NON_COMPLIANT.

Contexto: se considera que una política de función de Lambda permite el acceso público si el elemento principal está vacío o contiene un comodín. Por ejemplo, si el elemento principal es `“”` o `{“AWS”: “”}`. Por motivos de seguridad, no es recomendable conceder acceso público. Restringir el acceso público puede ayudarle a evitar las invocaciones no autorizadas de las funciones de Lambda, que podrían comprometer sus datos o generar costos no deseados.

Para restringir el acceso a las funciones de Lambda, especifique la AWS cuenta IDs o los nombres de los recursos de Amazon (ARNs) de los usuarios, roles o servicios de IAM que pueden invocar las funciones. Para obtener más información, consulte cómo otorgarles a otras cuentas el acceso a las funciones en la Guía del desarrollador de AWS Lambda .

La regla también es `NON_COMPLIANT` si se invoca una función de Lambda desde Amazon S3 y la política no incluye una condición para limitar el acceso público, como por ejemplo `AWS:SourceAccount`. Le recomendamos que utilice otras condiciones de S3 junto con `AWS:SourceAccount` en su política de bucket para obtener un acceso más preciso.

> **Note**
>
> Para que se considere no pública, una política basada en recursos de Lambda debe conceder acceso solo a valores fijos. Esto significa valores que no contienen un comodín ni el siguiente elemento de política de IAM: Variables.

Identificador: LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

Tipos de recursos: AWS::Lambda::Function

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto Europa (España) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

lambda-function-settings-check

Comprueba si la configuración de la función AWS Lambda para el tiempo de ejecución, la función, el tiempo de espera y el tamaño de la memoria coinciden con los valores esperados. La regla ignora las funciones con el tipo de paquete “Image” y las funciones con el tiempo de ejecución establecido en Tiempo de ejecución exclusivo del sistema operativo. La regla es NON_COMPLIANT si la configuración de la función de Lambda no coincide con los valores esperados.

Identificador: LAMBDA_FUNCTION_SETTINGS_CHECK

Tipos de recursos: AWS::Lambda::Function

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

tiempo de ejecución, Tipo: CSV

Lista de valores de tiempo de ejecución de Lambda AWS separados por comas

role (opcional), Tipo: cadena

Nombre o ARN de la función de ejecución de Lambda AWS

memorySize (opcional), Tipo: int, Valor predeterminado: 128

AWS Tamaño de la función Lambda en megabytes

timeout (opcional), Tipo: int, Valor predeterminado: 3

AWS Tiempo de espera de la función Lambda en segundos

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con AWS Config reglas. Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

* Para obtener más información sobre los valores válidos de estas entradas, consulte Rol MemorySize, tiempo de ejecución y tiempo de espera en la Guía del AWS CloudFormation usuario.

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

lambda-function-xray-enabled

Comprueba si AWS X-Ray está activado en las funciones de AWS Lambda. La regla no cumple con los requisitos si el trazado de rayos X está desactivado para una función Lambda.

Identificador: LAMBDA_FUNCTION_XRAY_ENABLED

Tipos de recursos: AWS::Lambda::Function

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

lambda-inside-vpc

Comprueba si una función de Lambda puede acceder a una nube privada virtual (VPC). La regla es NON_COMPLIANT si la función de Lambda no está activada en una VPC.

Identificador: LAMBDA_INSIDE_VPC

Tipos de recursos: AWS::Lambda::Function

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

subnetIds (opcional), Tipo: CSV

Lista de subredes separadas por comas a las que deben IDs estar asociadas las funciones de Lambda.

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con reglas. AWS Config Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

lambda-vpc-multi-az-comprobar

Comprueba si Lambda tiene asociada más de una zona de disponibilidad. La regla es NON_COMPLIANT si solo hay una zona de disponibilidad asociada a Lambda o si el número de zonas de disponibilidad asociadas es inferior al número especificado en el parámetro opcional.

Identificador: LAMBDA_VPC_MULTI_AZ_CHECK

Tipos de recursos: AWS::Lambda::Function

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

availabilityZones (opcional), Tipo: int

Número previsto de zonas de disponibilidad.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

lightsail-bucket-allow-public- anula - desactivado

Comprueba si los buckets de Amazon Lightsail tienen deshabilitada la opción de anulación pública. Si es verdadera, la regla no cumple con las normas. AllowPublicOverrides Nota: no AllowPublicOverrides tiene ningún efecto si GetObject es pública, consulte lightsail-bucket-get-object -private.

Identificador: LIGHTSAIL_BUCKET_ALLOW_PUBLIC_OVERRIDES_DISABLED

Tipos de recursos: AWS::Lightsail::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

lightsail-bucket-tagged

Comprueba si los cubos de Amazon Lightsail tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: LIGHTSAIL_BUCKET_TAGGED

Tipos de recursos: AWS::Lightsail::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

lightsail-certificate-tagged

Comprueba si los certificados de Amazon Lightsail tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: LIGHTSAIL_CERTIFICATE_TAGGED

Tipos de recursos: AWS::Lightsail::Certificate

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

lightsail-disk-tagged

Comprueba si los discos de Amazon Lightsail tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: LIGHTSAIL_DISK_TAGGED

Tipos de recursos: AWS::Lightsail::Disk

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

macie-auto-sensitive-data-comprobación-descubrimiento

Comprueba si la detección automatizada de datos confidenciales está habilitada en Amazon Macie. La regla es NON_COMPLIANT si la detección automatizada de datos confidenciales está deshabilitada. La regla es APPLICABLE para las cuentas de administrador y NOT_APPLICABLE para las cuentas de los miembros.

Identificador: MACIE_AUTO_SENSITIVE_DATA_DISCOVERY_CHECK

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningun Xia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

macie-status-check

Comprueba si Amazon Macie está activado en su cuenta por región. La regla es NON_COMPLIANT si el atributo Status no se ha definido como ENABLED.

Identificador: MACIE_STATUS_CHECK

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

mariadb-publish-logs-to-registros de cloudwatch

Comprueba si las instancias de base de datos de Amazon MariaDB están configuradas para publicar registros en Amazon Logs. CloudWatch La regla no es compatible si una instancia de base de datos no está configurada para publicar registros en Logs. CloudWatch

Identificador: MARIADB_PUBLISH_LOGS_TO_CLOUDWATCH_LOGS

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

logTypes (opcional), Tipo: cadena

Lista separada por comas de tipos de registros que la regla debe comprobar. Si no se proporciona, la regla comprueba los tipos de registros predeterminados: “error” y “auditoría”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

mfa-enabled-for-iam-acceso a la consola

Comprueba si la autenticación AWS multifactor (MFA) está habilitada para AWS todos los usuarios de Identity and Access Management (IAM) Access Management que utilizan una contraseña de consola. La regla es COMPLIANT si MFA está habilitado.

> **Note**
>
> Plazo de reevaluación
>
> Volver a evaluar esta regla en un plazo de 4 horas tras la primera evaluación no tendrá ningún efecto en los resultados.
>
> Reglas administradas y tipos de recursos de IAM globales
>
> Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.
>
> Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.
>
> A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones

compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Identificador: MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

Tipos de recursos: AWS::IAM::User

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

mq-active-broker-ldap-autenticación

Comprueba si los agentes de Amazon MQ ActiveMQ utilizan la estrategia de autenticación LDAP para proteger al agente. La regla NO ES COMPATIBLE si está configurada. AuthenticationStrategy no es «ldap».

Identificador: MQ_ACTIVE_BROKER_LDAP_AUTHENTICATION

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

mq-active-deployment-mode

Comprueba el modo de implementación configurado para el motor del agente ActiveMQ de Amazon MQ. La regla es NON_COMPLIANT si se utiliza el modo de agente de instancia única predeterminado.

Identificador: MQ_ACTIVE_DEPLOYMENT_MODE

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Centro), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

mq-active-single-instance-broker-storage-type-efs

Comprueba si un bróker de instancia única de Amazon MQ para ActiveMQ que utilice la familia de tipos de instancias mq.m5 está configurado con Amazon Elastic File System (EFS) para el

almacenamiento de agentes. La regla NO ES COMPATIBLE si está configurada. StorageType no es 'efs'.

Identificador: MQ_ACTIVE_SINGLE_INSTANCE_BROKER_STORAGE_TYPE_EFS

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

mq-automatic-minor-version-habilitado para la actualización

Comprueba si las actualizaciones automáticas de versiones secundarias están habilitadas para los agentes de Amazon MQ. La regla es NON_COMPLIANT si el campo 'AutoMinorVersionUpgrade' no está habilitado para un bróker de Amazon MQ.

Identificador: MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

mq-auto-minor-version-habilitado para la actualización

Comprueba si las actualizaciones automáticas de versiones secundarias están habilitadas para los agentes de Amazon MQ. La regla es NON_COMPLIANT si el campo 'AutoMinorVersionUpgrade' no está habilitado para un bróker de Amazon MQ.

Identificador: MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Centro), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

mq-broker-general-logging-habilitado

Comprueba si los agentes de Amazon MQ tienen habilitado el registro general. La regla es NON_COMPLIANT si configuration.Logs.General es False.

Identificador: MQ_BROKER_GENERAL_LOGGING_ENABLED

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

mq-cloudwatch-audit-logging-habilitado

Comprueba si los agentes de Amazon MQ tienen activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

Identificador: MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

mq-cloudwatch-audit-log-habilitado

Comprueba si un agente de Amazon MQ tiene activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

Identificador: MQ_CLOUDWATCH_AUDIT_LOG_ENABLED

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

mq-no-public-access

Comprueba si los agentes de Amazon MQ no son de acceso público. La regla es NON_COMPLIANT si el campo 'PubliclyAccessible' está establecido en true para un bróker de Amazon MQ.

Identificador: MQ_NO_PUBLIC_ACCESS

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Caledonia) Gary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

mq-rabbit-deployment-mode

Comprueba el modo de implementación configurado para el motor del agente RabbitMQ de Amazon MQ. La regla es NON_COMPLIANT si se utiliza el modo de agente de instancia única predeterminado.

Identificador: MQ_RABBIT_DEPLOYMENT_MODE

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

msk-cluster-public-access-deshabilitado

Comprueba si el acceso público está deshabilitado en los clústeres de Amazon MSK. La regla es NON_COMPLIANT si el acceso público a un clúster de Amazon MSK no está deshabilitado.

Identificador: MSK_CLUSTER_PUBLIC_ACCESS_DISABLED

Tipos de recursos: AWS::MSK::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

msk-cluster-tagged

Comprueba si los clústeres de Amazon MSK tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: MSK_CLUSTER_TAGGED

Tipos de recursos: AWS::MSK::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

msk-connect-connector-logging-habilitado

Comprueba si Amazon MSK Connector tiene habilitado el registro en alguno de los destinos de registro. La regla es NON_COMPLIANT si Amazon MSK Connector no tiene habilitado el registro.

Identificador: MSK_CONNECT_CONNECTOR_LOGGING_ENABLED

Tipos de recursos: AWS::KafkaConnect::Connector

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

msk-enhanced-monitoring-enabled

Comprueba si la supervisión mejorada está habilitada para un clúster de Amazon MSK establecido en PER_TOPIC_PER_BROKER o PER_TOPIC_PER_PARTITION. La regla es NON_COMPLIANT si la supervisión mejorada está habilitada y se establece en DEFAULT o PER_BROKER.

Identificador: MSK_ENHANCED_MONITORING_ENABLED

Tipos de recursos: AWS::MSK::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

msk-in-cluster-node-requerido-tls

Comprueba si un clúster de Amazon MSK está cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.

Identificador: MSK_IN_CLUSTER_NODE_REQUIRE_TLS

Tipos de recursos: AWS::MSK::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

msk-unrestricted-access-check

Comprueba si un clúster de Amazon MSK tiene deshabilitado el acceso no autenticado. La regla es NON_COMPLIANT si el clúster de Amazon MSK tiene habilitado el acceso no autenticado.

Identificador: MSK_UNRESTRICTED_ACCESS_CHECK

Tipos de recursos: AWS::MSK::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

multi-region-cloudtrail-enabled

> **Important**
>
> Para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled

Comprueba si hay al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el `ExcludeManagementEventSources` campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos o AWS KMS eventos de Amazon RDS Data API.

Identificador: MULTI_REGION_CLOUD_TRAIL_ENABLED

Tipo de disparador: periódico

Región de AWS: Todas las regiones compatibles AWS

Parámetros:

s3 BucketName (opcional), Tipo: cadena

Nombre del bucket de Amazon S3 AWS CloudTrail al que se van a entregar los archivos de registro.

snsTopicArn (Opcional), Tipo: cadena

El ARN del tema de Amazon SNS para usarlo en las notificaciones AWS CloudTrail .

cloudWatchLogsLogGroupArn (Opcional), Tipo: cadena

ARN del grupo de CloudWatch registros de Amazon AWS CloudTrail al que enviar datos.

includeManagementEvents (Opcional), Tipo: booleano

Selector de eventos para incluir los eventos de administración de AWS CloudTrail.

readWriteType (Opcional), Tipo: cadena

Tipo de eventos que registrar. Los valores válidos son ReadOnly, WriteOnly y TODOS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

nacl-no-unrestricted-ssh-rdp

Comprueba si los puertos predeterminados para el tráfico de SSH/RDP entrada de las listas de control de acceso a la red (NACLs) no están restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

Identificador: NACL_NO_UNRESTRICTED_SSH_RDP

Tipos de recursos: AWS::EC2::NetworkAcl

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

neptune-cluster-backup-retention-comprobar

Comprueba si el período de retención de un clúster de base de datos de Amazon Neptune está establecido en un número específico de días. La regla es NON_COMPLIANT si el período de retención es inferior al valor especificado por el parámetro.

Identificador: NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Región de Zúrich)

Parámetros:

minimumBackupRetentionPunto (opcional), Tipo: int

> Las copias de seguridad se deben conservar un mínimo de días. Los valores válidos son del 1 al 35; el valor predeterminado es 7. La regla no es compatible si el valor es mayor que ". backupRetentionPeriod La regla cumple con los requisitos si el valor es menor o igual a ". backupRetentionPeriod

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

neptune-cluster-cloudwatch-log-habilitado para exportación

Comprueba si un clúster de Amazon Neptune tiene habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.

Identificador: NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Región de Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

neptune-cluster-copy-tags-to-snapshot-enabled

Comprueba si un clúster de Amazon Neptune está configurado para copiar todas las etiquetas en instantáneas cuando se crean las instantáneas. La regla no es compatible si el valor de «Instantánea» copyTagsTo está establecido en false.

Identificador: NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Región de Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

neptune-cluster-deletion-protection-habilitado

Comprueba si un clúster de base de datos de Amazon Neptune tiene habilitada la protección contra eliminación. La regla es NON_COMPLIANT si un clúster de Amazon Neptune tiene el campo deletionProtection establecido en false.

Identificador: NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Región de Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

neptune-cluster-encrypted

Comprueba si el cifrado de almacenamiento está habilitado para los clústeres de base de datos de Amazon Neptune. La regla es NON_COMPLIANT si el cifrado de almacenamiento no está habilitado.

Identificador: NEPTUNE_CLUSTER_ENCRYPTED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Región de Zúrich)

Parámetros:

KmsKeyArns , Tipo: CSV

Una lista de claves de KMS separada por comas ARNs para compararla con la KmsKeyId del clúster cifrado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

neptune-cluster-iam-database-autenticación

Comprueba si un clúster de Amazon Neptune tiene habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.

Identificador: NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Región de Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

neptune-cluster-multi-az-habilitado

Comprueba si un clúster de Amazon Neptune está configurado con la replicación de Amazon RDS Multi-AZ. La regla es NON_COMPLIANT si la replicación Multi-AZ no está habilitada.

Identificador: NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Región de Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

neptune-cluster-snapshot-encrypted

Comprueba si un clúster de base de datos de Amazon Neptune tiene instantáneas cifradas. La regla es NON_COMPLIANT si un clúster de Neptune no tiene las instantáneas cifradas.

Identificador: NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

Tipos de recursos: AWS::RDS::DBClusterSnapshot

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

neptune-cluster-snapshot-public-prohibido

Comprueba si una instantánea manual de un clúster de base de datos de Amazon Neptune es pública. La regla es NON_COMPLIANT si las instantáneas de clústeres nuevas y existentes de Neptune son públicas.

Identificador: NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

Tipos de recursos: AWS::RDS::DBClusterSnapshot

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

netfw-deletion-protection-enabled

Comprueba si AWS Network Firewall tiene habilitada la protección contra eliminaciones. La regla es NON_COMPLIANT si un clúster de Network Firewall no tiene habilitada la protección contra eliminación.

Identificador: NETFW_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::NetworkFirewall::Firewall

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

netfw-logging-enabled

Comprueba si los firewalls de AWS Network Firewall tienen habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

Identificador: NETFW_LOGGING_ENABLED

Tipos de recursos: AWS::NetworkFirewall::LoggingConfiguration

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

logType (opcional), Tipo: cadena

logType (opcional): tipo de registro para la regla que comprueba los firewalls: alert, flow o both.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

netfw-multi-az-enabled

Comprueba si los firewalls de AWS Network Firewall están desplegados en varias zonas de disponibilidad. La regla es NON_COMPLIANT si los firewalls se implementan en una sola zona de disponibilidad o en menos zonas que el número indicado en el parámetro opcional.

Identificador: NETFW_MULTI_AZ_ENABLED

Tipos de recursos: AWS::NetworkFirewall::Firewall

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

availabilityZones (opcional), Tipo: int

Número previsto de zonas de disponibilidad.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

netfw-policy-default-action-paquetes de fragmentos

Comprueba si una política AWS de Network Firewall está configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmentados. La regla es NON_COMPLIANT si la acción predeterminada sin estado para los paquetes fragmentados no coincide con la acción predeterminada definida por el usuario.

Identificador: NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

Tipos de recursos: AWS::NetworkFirewall::FirewallPolicy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

statelessFragmentDefaultAcciones, Tipo: CSV

Lista separada por comas de los valores. Puede seleccionar un máximo de dos. Los valores válidos son aws:pass, aws:drop y aws:forward_to_sfe.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

netfw-policy-default-action-paquetes completos

Comprueba si una política AWS de Network Firewall está configurada con una acción sin estado predeterminada definida por el usuario para los paquetes completos. La regla es NON_COMPLIANT si la acción predeterminada sin estado para los paquetes completos no coincide con la acción predeterminada sin estado definida por el usuario.

Identificador: NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

Tipos de recursos: AWS::NetworkFirewall::FirewallPolicy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

statelessDefaultActions, Tipo: CSV

Lista separada por comas de los valores. Puede seleccionar un máximo de dos. Los valores válidos son aws:pass, aws:drop y aws:forward_to_sfe.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

netfw-policy-rule-group-asociado

Compruebe que la política de AWS Network Firewall esté asociada a grupos de reglas con estado o sin estado. Esta regla es NON_COMPLIANT si no hay grupos de reglas con o sin estado asociados a la política de Network Firewall; de lo contrario, es COMPLIANT si existe alguno de los grupos de reglas.

Identificador: NETFW_POLICY_RULE_GROUP_ASSOCIATED

Tipos de recursos: AWS::NetworkFirewall::FirewallPolicy

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

netfw-stateless-rule-group-no está vacío

Comprueba si un grupo de reglas de firewall de red sin estado contiene reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas de firewall de red sin estado.

Identificador: NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

Tipos de recursos: AWS::NetworkFirewall::RuleGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

netfw-subnet-change-protection-habilitado

Comprueba si AWS Network Firewall tiene habilitada la protección contra cambios de subred. La regla es NON_COMPLIANT si la protección contra cambios en la subred no está habilitada.

Identificador: NETFW_SUBNET_CHANGE_PROTECTION_ENABLED

Tipos de recursos: AWS::NetworkFirewall::Firewall

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

nlb-cross-zone-load-habilitado para el equilibrio

Comprueba si el equilibrio de carga entre zonas está activado en los balanceadores de carga de red (). NLBs La regla es NON_COMPLIANT si el equilibrio de carga entre zonas no está habilitado para un NLB.

Identificador: NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

nlb-internal-scheme-check

Comprueba si un esquema del Equilibrador de carga de red es interno. La regla es NON_COMPLIANT si el esquema de configuración no se establece como interno.

Identificador: NLB_INTERNAL_SCHEME_CHECK

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

nlb-listener-tagged

Comprueba si los oyentes del Equilibrador de carga de red tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: NLB_LISTENER_TAGGED

Tipos de recursos: AWS::ElasticLoadBalancingV2::Listener

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

nlb-logging-enabled

Comprueba si el registro de acceso está habilitado para los equilibradores de carga de red. La regla es NON_COMPLIANT si el registro de acceso no está habilitado para un equilibrador de carga de red.

Identificador: NLB_LOGGING_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

nlb-tagged

Comprueba si los equilibradores de carga de red tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: NLB_TAGGED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

no-unrestricted-route-to-igw

Comprueba si hay rutas públicas en la tabla de enrutamiento a una puerta de enlace de Internet (IGW). La regla es NON_COMPLIANT si una ruta hacia una IGW tiene un bloque CIDR de destino 0.0.0.0/0 o ::/0 o si un bloque CIDR de destino no coincide con el parámetro de la regla.

Identificador: NO_UNRESTRICTED_ROUTE_TO_IGW

Tipos de recursos: AWS::EC2::RouteTable

Tipo de desencadenador: cambios de configuración y periódicos

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

routeTableIds (Opcional), Tipo: CSV

Lista de tablas de rutas separadas por comas IDs que pueden tener rutas a un Internet Gateway con un bloque CIDR de destino de '0.0.0.0/0' o ': :/0'.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

opensearch-access-control-enabled

Comprueba si los dominios OpenSearch de Amazon Service tienen activado el control de acceso detallado. La regla no es conforme si no está habilitada para AdvancedSecurityOptions el dominio del servicio. OpenSearch

Identificador: OPENSEARCH_ACCESS_CONTROL_ENABLED

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

opensearch-audit-logging-enabled

Comprueba si los dominios OpenSearch de Amazon Service tienen activado el registro de auditoría. La regla no cumple con los requisitos si un dominio de OpenSearch servicio no tiene activado el registro de auditoría.

Identificador: OPENSEARCH_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico

(Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

cloudWatchLogsLogGroupArnList (Opcional), Tipo: CSV

> Lista de nombres de recursos de Amazon (ARNs) separados por comas para los grupos de CloudWatch registros de Amazon Logs. La regla comprueba si los grupos de registros especificados están configurados para los registros de auditoría.
>
> Los valores válidos incluyen: `arn:aws:logs:region:account-id:log-group:log_group_name:*` y `arn:aws:logs:region:account-id:log-group:log_group_name`.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

opensearch-data-node-fault-tolerancia

Comprueba si los dominios OpenSearch de Amazon Service están configurados con al menos tres nodos de datos y zoneAwarenessEnabled es verdadero. La regla es NON_COMPLIANT para un OpenSearch dominio si «instanceCount» es inferior a 3 o si «» se establece como «false». zoneAwarenessEnabled

Identificador: OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

opensearch-encrypted-at-rest

Comprueba si los dominios OpenSearch de Amazon Service tienen habilitada la configuración de cifrado en reposo. La regla es NON_COMPLIANT si el campo `EncryptionAtRestOptions` no está habilitado.

> **Note**
>
> La regla no evalúa los dominios de Elasticsearch.

Identificador: OPENSEARCH_ENCRYPTED_AT_REST

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

opensearch-https-required

Comprueba si las conexiones a los dominios utilizan HTTPS OpenSearch . La regla no es conforme si el OpenSearch dominio de Amazon «EnforceHttps» no es «true» o es «true» y «TLSSecurityPolicy» no está en «». `tlsPolicies`

Identificador: OPENSEARCH_HTTPS_REQUIRED

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

tlsPolicies (opcional), Tipo: CSV

> Lista de políticas de seguridad de TLS separadas por comas para compararlas con el dominio de Amazon. OpensSearch

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

opensearch-in-vpc-only

Comprueba si los dominios OpenSearch de Amazon Service están en una Amazon Virtual Private Cloud (VPC). La regla no cumple con los requisitos si el punto final de un dominio OpenSearch de servicio es público.

> **Note**
>
> La regla no evalúa los dominios de Elasticsearch.

Identificador: OPENSEARCH_IN_VPC_ONLY

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

opensearch-logs-to-cloudwatch

Comprueba si los dominios OpenSearch de Amazon Service están configurados para enviar registros a Amazon CloudWatch Logs. La regla es NON_COMPLIANT si el registro no está configurado.

> **Note**
>
> La regla no evalúa los dominios de Elasticsearch.

Identificador: OPENSEARCH_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS

GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

logTypes (opcional), Tipo: CSV

Lista separada por comas de los registros que están habilitados. Los valores válidos son search, index y error.

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

opensearch-node-to-node-comprobación de cifrado

Comprueba si los nodos OpenSearch de Amazon Service están cifrados de extremo a extremo. La regla no cumple con los requisitos si el node-to-node cifrado no está activado en el dominio

> **Note**
> La regla no evalúa los dominios de Elasticsearch.

Identificador: OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

opensearch-primary-node-fault-tolerancia

Comprueba si los dominios OpenSearch de Amazon Service están configurados con al menos tres nodos principales dedicados. La regla no cumple con los requisitos para un dominio de OpenSearch servicio si DedicatedMasterEnabled «» se establece en «falso» o «DedicatedMasterCount» es inferior a 3.

Identificador: OPENSEARCH_PRIMARY_NODE_FAULT_TOLERANCE

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

opensearch-update-check

Comprueba si las actualizaciones de las versiones de Amazon OpenSearch Service están disponibles pero no están instaladas. La regla no cumple con los requisitos para un OpenSearch dominio si las últimas actualizaciones de software no están instaladas.

Identificador: OPENSEARCH_UPDATE_CHECK

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rabbit-mq-supported-version

Comprueba si un agente de RabbitMQ de Amazon MQ se ejecuta en una versión de motor mínima compatible que se haya especificado. La regla es NON_COMPLIANT si el agente de RabbitMQ no se ejecuta en la versión de motor mínima compatible que usted especifique.

Identificador: RABBIT_MQ_SUPPORTED_VERSION

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

supportedEngineVersion, Tipo: cadena

> Valor de cadena de la regla para comprobar la versión de motor mínima compatible para el agente de RabbitMQ. Los agentes de RabbitMQ utilizan la especificación semántica de control de versiones X.Y.Z. X indica la versión principal, Y representa la versión secundaria y Z representa la versión del parche.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-aurora-mysql-audit-habilitado para el registro

Comprueba si los clústeres de Amazon Aurora Compatible Edition con MySQL están configurados para publicar registros de auditoría en Amazon Logs. CloudWatch La regla es NON_COMPLIANT si los clústeres de la edición compatible con Aurora MySQL no tienen habilitada la publicación de registros de auditoría.

Identificador: RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-aurora-postgresql-logs-a Cloudwatch

Comprueba si un clúster de base de datos PostgreSQL de Amazon Aurora está configurado para publicar registros de PostgreSQL en Amazon Logs. CloudWatch Esta regla no cumple con los requisitos si el clúster de base de datos no está configurado para publicar registros de PostgreSQL en Amazon Logs. CloudWatch

Identificador: RDS_AURORA_POSTGRESQL_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región Europa (España)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-automatic-minor-version-habilitado para la actualización

Comprueba si las instancias de base de datos de Amazon Relational Database Service (RDS) están configuradas para las actualizaciones de versiones secundarias automáticas. La regla no es compatible si el valor de «Actualización» es falso. autoMinorVersion

Identificador: RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con reglas. AWS Config Para que esta regla devuelva COMPLIANT en modo proactivo, el

esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

* Para obtener más información sobre los valores válidos de estas entradas, consulte AutoMinorVersionUpgrade el motor en la Guía del AWS CloudFormation usuario.

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-cluster-auto-minor-version-upgrade-enable

Comprueba si las actualizaciones automáticas de versiones secundarias están habilitadas para las implementaciones de clústeres de Amazon RDS Multi-AZ. La regla no es compatible si la autoMinorVersion actualización está establecida en False.

Identificador: RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), EE. UU. Oeste (Norte de California), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-cluster-default-admin-comprobar

Comprueba si un clúster de base de datos de Amazon Relational Database Service (Amazon RDS) ha modificado el valor predeterminado del nombre de usuario de administrador. La regla es NON_COMPLIANT si el nombre de usuario de administrador está establecido en el valor predeterminado.

Identificador: RDS_CLUSTER_DEFAULT_ADMIN_CHECK

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary) y China (Ningxia) región AWS GovCloud

Parámetros:

validAdminUserNombres (opcionales), Tipo: CSV

> Lista separada por comas de los nombres de usuario de administrador que pueden usar los clústeres de Amazon RDS. Los nombres de usuario postgres o admin no son válidos, pues son valores predeterminados.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-cluster-deletion-protection-habilitado

Comprueba si un clúster de Amazon Relational Database Service (Amazon RDS) tiene habilitada la protección contra eliminación. La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la protección contra eliminación.

Identificador: RDS_CLUSTER_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-cluster-encrypted-at-descanso

Comprueba si un clúster de Amazon Relational Database Service (Amazon RDS) está cifrado en reposo. La regla es NON_COMPLIANT si el clúster de Amazon RDS no está cifrado en reposo.

Identificador: RDS_CLUSTER_ENCRYPTED_AT_REST

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-cluster-iam-authentication-habilitado

Comprueba si un clúster de Amazon Relational Database Service (Amazon RDS) AWS tiene habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.

Identificador: RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rds-cluster-multi-az-habilitado

Comprueba si la replicación en zonas de disponibilidad múltiple (Multi-AZ) está habilitada en los clústeres de Amazon Aurora y Multi-AZ DB administrados por Amazon Relational Database Service (Amazon RDS). La regla es NON_COMPLIANT si una instancia de Amazon RDS no está configurada con Multi-AZ.

Identificador: RDS_CLUSTER_MULTI_AZ_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-db-security-group-no permitido

Comprueba si hay algún grupo de seguridad de base de datos de Amazon Relational Database Service (Amazon RDS) que no sea el grupo de seguridad de base de datos predeterminado. La regla es NON_COMPLIANT si hay algún grupo de seguridad de base de datos que no sea el grupo de seguridad de base de datos predeterminado.

Identificador: RDS_DB_SECURITY_GROUP_NOT_ALLOWED

Tipos de recursos: AWS::RDS::DBSecurityGroup

Tipo de disparador: cambios de configuración

Región de AWS: solo disponible en Europa (Irlanda), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-enhanced-monitoring-enabled

Comprueba si las instancias de Amazon RDS tienen habilitado el monitoreo mejorado. Esta regla es NON_COMPLIANT si `monitoringInterval` es 0 en el elemento de configuración de la instancia de RDS o si `monitoringInterval` no coincide con el valor del parámetro de la regla.

Identifier (Identificador): RDS_ENHANCED_MONITORING_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

monitoringInterval (opcional), Tipo: int

> Valor entero en segundos entre puntos cuando se recopilan métricas de monitoreo mejoradas para la instancia de base de datos. Los valores válidos son 1, 5, 10, 15, 30 y 60.

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con AWS Config reglas. Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

* Para obtener más información sobre los valores válidos de estas entradas, consulte MonitoringIntervalel motor en la Guía del AWS CloudFormation usuario.

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-event-subscription-tagged

Comprueba si las suscripciones a eventos de Amazon RDS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: RDS_EVENT_SUBSCRIPTION_TAGGED

Tipos de recursos: AWS::RDS::EventSubscription

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-instance-default-admin-comprobar

Comprueba si una base de datos de Amazon Relational Database Service (Amazon RDS) ha modificado el valor predeterminado del nombre de usuario de administrador. Esta regla solo se

ejecutará en las instancias de bases de datos de RDS. La regla es NON_COMPLIANT si el nombre de usuario de administrador está establecido en el valor predeterminado.

Identificador: RDS_INSTANCE_DEFAULT_ADMIN_CHECK

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

validAdminUserNombres (opcionales), Tipo: CSV

> Lista separada por comas de los nombres de usuario de administrador que pueden usar las instancias de Amazon RDS. (Los nombres de usuario postgres o admin no son válidos, pues son valores predeterminados).

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rds-instance-deletion-protection-habilitado

Comprueba si una instancia de Amazon Relational Database Service (Amazon RDS) tiene habilitada la protección contra eliminación. La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la protección contra eliminación; por ejemplo, deletionProtection se establece en false.

> **Warning**
>
> Algunas instancias de bases de datos de RDS dentro de un clúster (Aurora/DocumentDB) se mostrarán como no conformes.

Identificador: RDS_INSTANCE_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

databaseEngines (opcional), Tipo: CSV

> Lista separada por comas de motores de base de datos de RDS que se deben incluir en la evaluación de la regla. Por ejemplo, mysql, postgres y mariadb.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rds-instance-iam-authentication-habilitado

Comprueba si una instancia de Amazon Relational Database Service (Amazon RDS) AWS tiene habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.

> **Note**
>
> El motor de base de datos debe ser uno de los siguientes: mysql, postgres, aurora, aurora-mysql o aurora-postgresql. El estado de la instancia de base de datos debe ser available, backing-up, storage-optimization o storage-full.

Identificador: RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-instance-public-access-comprobar

Comprueba si las instancias de Amazon Relational Database Service (Amazon RDS) no son de acceso público. La regla es NON_COMPLIANT si el campo publiclyAccessible es true en el elemento de configuración de instancia.

Identificador: RDS_INSTANCE_PUBLIC_ACCESS_CHECK

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con reglas. AWS Config Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-instance-subnet-igw-comprobar

Comprueba si las instancias de RDS DB están implementadas en una subred pública con una ruta a la puerta de enlace de Internet. La regla es NON_COMPLIANT si las instancias de RDS DB se implementan en una subred pública

Identificador: RDS_INSTANCE_SUBNET_IGW_CHECK

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-in-backup-plan

Comprueba si las bases de datos de Amazon Relational Database Service (Amazon RDS) están presentes en los planes de AWS Backup. La regla no es conforme si las bases de datos de Amazon RDS no están incluidas en ningún plan de Backup AWS .

> **Note**
>
> La regla solo se aplica a las instancias de base de datos de Amazon Aurora. No se admiten los clústeres de base de datos.

Identificador: RDS_IN_BACKUP_PLAN

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rds-last-backup-recovery-punto creado

Comprueba si se ha creado un punto de recuperación para Amazon Relational Database Service (Amazon RDS). La regla es NON_COMPLIANT si la instancia de Amazon RDS no tiene ningún punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de las instancias de Amazon RDS para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID de la instancia de Amazon RDS que debe comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-logging-enabled

Comprueba si los registros respectivos de Amazon Relational Database Service (Amazon RDS) están habilitados. La regla es NON_COMPLIANT si los tipos de registro no están habilitados.

> **Note**
>
> Las instancias de base de datos que no tengan el estado available, backing-up, storage-optimization o storage-full se evalúan como `NOT_APPLICABLE`.

Identificador: RDS_LOGGING_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

additionalLogs (opcional), Tipo: StringMap

Lista separada por comas de nombres de motor y de tipo de registro. Por ejemplo, "additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-mariadb-instance-encrypted-en tránsito

Comprueba si las conexiones a las instancias de Amazon RDS para MariaDB DB con una versión de motor superior o igual a 10.5 utilizan cifrado en tránsito. La regla es NON_COMPLIANT si el grupo de parámetros de DB asociado no está sincronizado o si el parámetro require_secure_transport no está establecido en ON.

Identificador: RDS_MARIADB_INSTANCE_ENCRYPTED_IN_TRANSIT

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-meets-restore-time-objetivo

Comprueba si el tiempo de restauración de las instancias de Amazon Relational Database Service (Amazon RDS) cumple con la duración especificada. La regla es NON_COMPLIANT si LatestRestoreExecutionTimeMinutes una instancia de Amazon RDS es superior a minutos. maxRestoreTime

Identificador: RDS_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

maxRestoreTime, Tipo: int

Valor numérico del tiempo de ejecución de restauración máximo permitido.

resourceTags (opcional), Tipo: cadena

Etiquetas de las instancias de Amazon RDS para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID de la instancia de Amazon RDS que debe comprobar la regla.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-multi-az-support

Comprueba si la alta disponibilidad está habilitada para sus instancias de base de datos de RDS.

En una implementación multi-AZ, Amazon RDS aprovisiona y mantiene automáticamente una réplica en espera sincrónica dentro de una zona de disponibilidad diferente. Para obtener más información, consulte Alta disponibilidad (Multi-AZ) en la Guía del usuario de Amazon RDS.

> **Note**
>
> Esta regla no evalúa las instancias de base de datos de Amazon Aurora, Amazon DocumentDB ni Amazon Neptune.

Identificador: RDS_MULTI_AZ_SUPPORT

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con reglas. AWS Config Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

* Para obtener más información sobre los valores válidos para estas entradas, consulte MultiAZ y Engine en la Guía del AWS CloudFormation usuario.

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-mysql-cluster-copy-tags-to-snapshot-check

Comprueba si los clústeres de MySQL DB de Amazon Relational Database Service (Amazon RDS) están configurados para copiar etiquetas en instantáneas. La regla es NON_COMPLIANT si el clúster de MySQL DB de Amazon RDS no está configurado para copiar etiquetas en instantáneas.

Identificador: RDS_MYSQL_CLUSTER_COPY_TAGS_TO_SNAPSHOT_CHECK

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Centro), EE. UU. Oeste (Norte de California) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-mysql-instance-encrypted-en tránsito

Comprueba si las conexiones a las instancias de bases de datos de Amazon RDS para MySQL están configuradas para utilizar el cifrado en tránsito. La regla es NON_COMPLIANT si el grupo de parámetros de base de datos asociado no está sincronizado o si el parámetro require_secure_transport no está establecido en 1.

> **Note**
>
> La regla se devuelve `NOT_APPLICABLE` si la instancia de Amazon RDS forma parte de un clúster de RDS.

identificador: RDS_MYSQL_INSTANCE_ENCRYPTED_IN_TRANSIT

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rds-option-group-tagged

Comprueba si los recursos del grupo de opciones de Amazon RDS tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: RDS_OPTION_GROUP_TAGGED

Tipos de recursos: AWS::RDS::OptionGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rds-pgsql-cluster-copy-tags-to-snapshot-check

Comprueba si los clústeres de PostgreSQL DB de Amazon Relational Database Service (Amazon RDS) están configurados para copiar etiquetas en instantáneas. La regla es NON_COMPLIANT si la propiedad de un clúster CopyTagsToSnapshot de base de datos PostgreSQL de RDS está establecida en false.

Identificador: RDS_PGSQL_CLUSTER_COPY_TAGS_TO_SNAPSHOT_CHECK

Tipos de recursos: AWS::RDS::DBCluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Centro), EE. UU. Oeste (Norte de California) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rds-postgresql-logs-to- vigilancia en la nube

Comprueba si una instancia de base de datos de Amazon PostgreSQL está configurada para publicar registros en Amazon Logs. CloudWatch La regla es NON_COMPLIANT si la instancia de base de datos no está configurada para publicar registros en Amazon CloudWatch Logs.

Identificador: RDS_POSTGRESQL_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

logTypes (opcional), Tipo: CSV

Lista de tipos de registros separados por comas que se publicarán en Logs. CloudWatch Los valores válidos son “postgresql” y “upgrade”. El valor predeterminado es “postgresql”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rds-postgres-instance-encrypted-en tránsito

Comprueba si las conexiones a las instancias de bases de datos de Amazon RDS para PostgreSQL están configuradas para utilizar el cifrado en tránsito. La regla es NON_COMPLIANT si el grupo de parámetros de base de datos asociado no está sincronizado o si el parámetro rds.force_ssl no está establecido en 1.

> **Note**
>
> La regla se devuelve `NOT_APPLICABLE` si la instancia de Amazon RDS forma parte de un clúster de RDS.

Identificador: RDS_POSTGRES_INSTANCE_ENCRYPTED_IN_TRANSIT

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-proxy-tls-encryption

Comprueba si los Amazon RDS Proxy aplican TLS para todas las conexiones. La regla es NON_COMPLIANT si un Amazon RDS Proxy no aplica TLS para todas las conexiones.

Identificador: RDS_PROXY_TLS_ENCRYPTION

Tipos de recursos: AWS::RDS::DBProxy

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-resources-protected-by-plan de respaldo

Comprueba si las instancias de Amazon Relational Database Service (Amazon RDS) están protegidas por un plan de copia de seguridad. La regla es NON_COMPLIANT si la instancia de Amazon RDS no está cubierta por un plan de copia de seguridad.

Identificador: RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de las instancias de Amazon RDS para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID de la instancia de Amazon RDS que debe comprobar la regla.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-snapshots-public-prohibited

Comprueba si las instantáneas de Amazon Relational Database Service (Amazon RDS) son públicas. La regla es NON_COMPLIANT si las instantáneas nuevas y existentes de Amazon RDS son públicas.

> **Note**
>
> La captura de resultados de conformidad puede demorar hasta 12 horas.

Identificador: RDS_SNAPSHOTS_PUBLIC_PROHIBITED

Tipos de recursos: AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), África (Ciudad del Cabo), Asia Pacífico (Melbourne), Europa (Milán), AWS GovCloud (EEUU-Este), AWS GovCloud (EEUU-Oeste), México (Centro), Israel (Tel Aviv), Asia Pacífico (Taipéi), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-snapshot-encrypted

Comprueba si las instantáneas de base de datos de Amazon Relational Database Service (Amazon RDS) están cifradas. La regla es NON_COMPLIANT si las instantáneas de base de datos de Amazon RDS no están cifradas.

Identificador: RDS_SNAPSHOT_ENCRYPTED

Tipos de recursos: AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rds-sqlserver-encrypted-in-tránsito

Comprueba si las conexiones a instancias de base de datos del servidor de SQL de Amazon RDS están configuradas para utilizar cifrado en tránsito. La regla no es compatible si el parámetro de base de datos force_ssl del grupo de parámetros no está establecido en 1 o si el parámetro no está «sincronizado». ApplyStatus

Identificador: RDS_SQLSERVER_ENCRYPTED_IN_TRANSIT

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-sql-server-logs-a Cloudwatch

Comprueba si una instancia de base de datos de Amazon SQL Server está configurada para publicar registros en Amazon CloudWatch Logs. Esta regla no es compatible si la instancia de base de datos no está configurada para publicar registros en Amazon CloudWatch Logs.

Identificador: RDS_SQL_SERVER_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

logTypes (opcional), Tipo: CSV

> LogTypes: (opcional): lista de tipos de registros separados por comas que se publicarán en Logs. CloudWatch Los valores válidos son “error” y “agent”. El valor predeterminado es “error” y “agent”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

rds-storage-encrypted

Comprueba si el cifrado de almacenamiento está activado para las instancias de base de datos de Amazon Relational Database Service (Amazon RDS). La regla es NON_COMPLIANT si el cifrado de almacenamiento no está habilitado.

Identificador: RDS_STORAGE_ENCRYPTED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

kmsKeyId (Opcional), Tipo: cadena

ID o nombre de recurso de Amazon (ARN) de clave de KMS que se utiliza para cifrar el almacenamiento.

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con AWS Config reglas. Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-audit-logging-enabled

Comprueba si los clústeres de Amazon Redshift registran auditorías en un bucket específico. La regla es NON_COMPLIANT si el registro de auditoría no está habilitado para un clúster de Redshift o si se proporciona el parámetro `bucketNames` pero el destino del registro de auditoría no coincide.

Identificador: REDSHIFT_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

bucketNames (opcional), Tipo: CSV

Lista separada por comas de los nombres de bucket de Amazon S3 para almacenar registros de auditoría.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

redshift-backup-enabled

Comprueba si las instantáneas automatizadas de Amazon Redshift están habilitadas para los clústeres. La regla es NON_COMPLIANT si el valor de `automatedSnapshotRetentionPeriod` es mayor que `MaxRetentionPeriod` o menor que `MinRetentionPeriod` o el valor es 0.

Identificador: REDSHIFT_BACKUP_ENABLED

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de México (Central)

Parámetros:

MinRetentionPeriod (Opcional), Tipo: int

Valor mínimo para el período de retención. El valor mínimo es 1.

MaxRetentionPeriod (Opcional), Tipo: int

Valor máximo para el período de retención. El valor máximo es 35.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-cluster-configuration-check

Comprueba si los clústeres de Amazon Redshift tienen la configuración especificada. La regla es NON_COMPLIANT si el clúster de Amazon Redshift no está cifrado o se cifra con otra clave, o si un clúster no tiene habilitado el registro de auditoría.

Identificador: REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de México (Central)

Parámetros:

loggingEnabled, Tipo: booleano, Predeterminado: true

El registro de auditoría está activado

clusterDbEncrypted, Tipo: booleano, Predeterminado: true

El cifrado de la base de datos está activado

nodeTypes (opcional), Tipo: CSV, Valor predeterminado: dc1.large

Especifique el tipo de nodo

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-cluster-kms-enabled

Comprueba si los clústeres de Amazon Redshift utilizan una clave AWS Key Management Service (AWS KMS) específica para el cifrado. La regla es COMPLIANT si el cifrado está activado y el clúster está cifrado con la clave proporcionada en el parámetro `kmsKeyArn`. La regla es NON_COMPLIANT si el clúster no está cifrado o está cifrado con otra clave.

Identificador: REDSHIFT_CLUSTER_KMS_ENABLED

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

> Lista separada por comas de los principales nombres de recursos de AWS KMS Amazon (ARNs) que se utilizan en los clústeres de Amazon Redshift para el cifrado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

redshift-cluster-maintenancesettings-check

Comprueba si los clústeres de Amazon Redshift tienen la configuración de mantenimiento especificada. La regla es NON_COMPLIANT si las actualizaciones automáticas a la versión principal están deshabilitadas.

Identificador: REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de México (Central)

Parámetros:

allowVersionUpgrade, Tipo: booleano, Predeterminado: true

Permite habilitar la actualización de la versión.

preferredMaintenanceWindow (Opcional), Tipo: cadena

Período de mantenimiento programado para clústeres (por ejemplo, Mon:09:30-Mon:10:00).

automatedSnapshotRetentionPeríodo (opcional), Tipo: int, Valor predeterminado: 1

Número de días durante los que se conservan las instantáneas automatizadas.

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con AWS Config reglas. Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

* Para obtener más información sobre los valores válidos de estas entradas AutomatedSnapshotRetentionPeriodPreferredMaintenanceWindow, consulte y AllowVersionUpgradeen la Guía del AWS CloudFormation usuario.

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-cluster-multi-az-habilitado

Comprueba si un clúster de Amazon Redshift tiene habilitadas implementaciones de múltiples zonas de disponibilidad. Esta regla es NON_COMPLIANT si el clúster de Amazon Redshift no tiene habilitadas implementaciones de múltiples zonas de disponibilidad.

Identificador: REDSHIFT_CLUSTER_MULTI_AZ_ENABLED

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), México (Central), EE.UU. Oeste (Norte de California) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

redshift-cluster-parameter-group-etiquetado

Comprueba si los grupos de parámetros de clúster de Amazon Redshift tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: REDSHIFT_CLUSTER_PARAMETER_GROUP_TAGGED

Tipos de recursos: AWS::Redshift::ClusterParameterGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-cluster-public-access-comprobar

Comprueba si los clústeres de Amazon Redshift no son de acceso público. La regla es NON_COMPLIANT si el campo publiclyAccessible es True en el elemento de configuración del clúster.

Identificador: REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Europa (Estocolmo), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con reglas. AWS Config Para que esta regla devuelva COMPLIANT en modo proactivo, el

esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-cluster-subnet-group-multifunción

Comprueba si los grupos de subredes de Amazon Redshift contienen subredes de varias zonas de disponibilidad. La regla es NON_COMPLIANT si un grupo de subredes de Amazon Redshift no contiene subredes de, al menos, dos zonas de disponibilidad distintas.

Identificador: REDSHIFT_CLUSTER_SUBNET_GROUP_MULTI_AZ

Tipos de recursos: AWS::Redshift::ClusterSubnetGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-default-admin-check

Comprueba si un clúster de Amazon Redshift ha cambiado el nombre de usuario de administrador con respecto a su valor predeterminado. La regla es NON_COMPLIANT si el nombre de usuario de administrador de un clúster de Redshift está definido como awsuser o si el nombre de usuario no coincide con lo que aparece en el parámetro.

Identificador: REDSHIFT_DEFAULT_ADMIN_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

validAdminUserNombres (opcionales), Tipo: CSV

> Lista separada por comas de los nombres de usuario de administrador que se pueden usar en los clústeres de Redshift. Nota: awsuser es el valor predeterminado y no se acepta.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

redshift-default-db-name-comprobar

Comprueba si un clúster de Redshift ha cambiado el nombre de la base de datos con respecto al valor predeterminado. La regla es NON_COMPLIANT si el nombre de la base de datos de un clúster de Redshift está establecido en dev o si se proporciona el parámetro opcional y el nombre de la base de datos no coincide.

Identificador: REDSHIFT_DEFAULT_DB_NAME_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

validDatabaseNames (Opcional), Tipo: CSV

Lista separada por comas de los nombres de base de datos para los clústeres de Redshift.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-enhanced-vpc-routing-habilitado

Comprueba si el clúster de Amazon Redshift tiene 'enhancedVpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRouting' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

Identificador: REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Europa (Estocolmo), China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-require-tls-ssl

Comprueba si los clústeres de Amazon Redshift requieren TLS/SSL cifrado para conectarse a los clientes de SQL. La regla es NON_COMPLIANT si un clúster de Amazon Redshift no tiene el parámetro require_SSL establecido en true.

Identificador: REDSHIFT_REQUIRE_TLS_SSL

Tipos de recursos: AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles, excepto la región de México (Central)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

redshift-serverless-default-admin-comprobar

Comprueba si un espacio de nombres de Amazon Redshift sin servidor ha cambiado el nombre de usuario de administrador con respecto a su valor predeterminado. La regla es NON_COMPLIANT si el nombre de usuario de administrador de un espacio de nombres de Redshift sin servidor está definido como “admin”.

Identificador: REDSHIFT_SERVERLESS_DEFAULT_ADMIN_CHECK

Tipos de recursos: AWS::RedshiftServerless::Namespace

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka),

Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), México (Central), Asia Pacífico (Taipéi), Región Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-serverless-default-db-verificación de nombres

Comprueba si un espacio de nombres de Amazon Redshift sin servidor ha cambiado el nombre de su base de datos con respecto a su valor predeterminado. La regla es NON_COMPLIANT si el nombre de la base de datos de un espacio de nombres de Amazon Redshift sin servidor se establece en “dev”.

Identificador: REDSHIFT_SERVERLESS_DEFAULT_DB_NAME_CHECK

Tipos de recursos: AWS::RedshiftServerless::Namespace

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), México (Central), Asia Pacífico (Taipéi), Región Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-serverless-namespace-cmk-cifrado

Comprueba si los espacios de nombres de Amazon Redshift Serverless están cifrados mediante claves de KMS administradas por el cliente. AWS La regla es NON_COMPLIANT si el espacio de nombres no está cifrado por una clave administrada por el cliente. También puede especificar claves de KMS que la regla debe comprobar.

Identificador: REDSHIFT_SERVERLESS_NAMESPACE_CMK_ENCRYPTION

Tipos de recursos: AWS::RedshiftServerless::Namespace

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), México (Central), Asia Pacífico (Taipéi), Región Canadá Oeste (Calgary)

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

> Lista separada por comas de los nombres de recursos de Amazon (ARNs) de claves gestionadas por el cliente para que la regla la compruebe. Si se proporciona, la regla es NON_COMPLIANT si el espacio de nombres de Amazon Redshift sin servidor no está cifrado con una de estas claves de KMS.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

redshift-serverless-publish-logs-a Cloudwatch

Comprueba si el espacio de nombres Amazon Redshift Serverless está configurado para publicar los siguientes registros en Amazon Logs. CloudWatch Esta regla no cumple con los requisitos si el espacio de nombres no está configurado para publicar los siguientes registros en Amazon Logs. CloudWatch

Identificador: REDSHIFT_SERVERLESS_PUBLISH_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::RedshiftServerless::Namespace

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EEUU-Este), (EEUU-Oeste) AWS GovCloud , México AWS GovCloud (Central), Asia Pacífico (Taipéi), Región Canadá Oeste (Calgary)

Parámetros:

logType (opcional), Tipo: CSV

> Lista separada por comas de los tipos de registro que se van a publicar en CloudWatch Logs. Los valores válidos son “connectionlog”, “userlog”. El valor predeterminado es “connectionlog”, “userlog”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

redshift-serverless-workgroup-encrypted-en tránsito

Comprueba si los grupos de trabajo sin servidor de AWS Redshift tienen el parámetro de configuración require_ssl establecido en true. La regla es NON_COMPLIANT si require_ssl es False.

Identificador: REDSHIFT_SERVERLESS_WORKGROUP_ENCRYPTED_IN_TRANSIT

Tipos de recursos: AWS::RedshiftServerless::Workgroup

Tipo de disparador: periódico

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney), Canadá (centro), Europa (España) y Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-serverless-workgroup-no-acceso público

Comprueba si los grupos de trabajo de Amazon Redshift sin servidor no permiten acceso público. La regla es NON_COMPLIANT si un grupo de trabajo tiene habilitado “Activar acceso público”.

Identificador: REDSHIFT_SERVERLESS_WORKGROUP_NO_PUBLIC_ACCESS

Tipos de recursos: AWS::RedshiftServerless::Workgroup

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Tailandia), África (Ciudad del Cabo), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (EEUU-Este), (EEUU-Oeste) AWS GovCloud , México (Central), Asia Pacífico AWS GovCloud (Taipéi), Canadá (Oeste Región de Calgary), China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

redshift-serverless-workgroup-routes-dentro del vpc

Comprueba si los grupos de trabajo de Amazon Redshift sin servidor enrutan el tráfico de red a través de una VPC. La regla es NON_COMPLIANT si los grupos de trabajo tienen deshabilitada “Activar enrutamiento de VPC mejorado”.

Identificador: REDSHIFT_SERVERLESS_WORKGROUP_ROUTES_WITHIN_VPC

Tipos de recursos: AWS::RedshiftServerless::Workgroup

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), África (Ciudad del Cabo), Oriente Medio (Emiratos Árabes Unidos), Sudamérica (São Paulo), Asia Pacífico (Hong Kong), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), Europa (Milán), (Región EEUU-Oeste) AWS GovCloud , México AWS GovCloud (Centro), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

redshift-unrestricted-port-access

Comprueba si los grupos de seguridad asociados a un clúster de Amazon Redshift tienen reglas de entrada que permiten el tráfico entrante sin restricciones. La regla es NON_COMPLIANT si hay reglas entrantes que permiten el tráfico entrante sin restricciones al puerto del clúster de Redshift.

Identificador: REDSHIFT_UNRESTRICTED_PORT_ACCESS

Tipos de recursos: AWS::Redshift::Cluster

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

required-tags

Comprueba si sus recursos tienen las etiquetas que ha especificado. Por ejemplo, puedes comprobar si tus EC2 instancias de Amazon tienen la `CostCenter` etiqueta y, al mismo tiempo, comprobar si todas tus instancias de RDS tienen un conjunto de etiquetas Keys. Separe los valores con comas. Puede comprobar hasta seis etiquetas a la vez.

Con AWS esta regla, el documento de AWS Systems Manager automatización gestionada `AWS-SetRequiredTags` no funciona como solución. Deberá crear su propia documentación de automatización de Systems Manager personalizada para la corrección.

Contexto: AWS permite asignar metadatos a los AWS recursos en forma de etiquetas. Cada etiqueta es una etiqueta que consta de una clave y un valor opcional para almacenar información sobre el recurso o los datos retenidos en ese recurso. Para obtener más información, consulte Creación de la estrategia de etiquetado.

Puede usar esta regla para buscar recursos en su cuenta que no se hayan lanzado con las configuraciones deseadas especificando qué recursos deben tener etiquetas y el valor esperado para cada etiqueta. También puede ejecutar acciones correctivas para corregir los errores en las etiquetas. Sin embargo, esta regla no impide crear recursos con etiquetas incorrectas.

> **Note**
>
> AWS Config no admite el registro de las etiquetas asociadas a todos los tipos de recursos. Para comprobar si AWS Config registra etiquetas en el elemento de configuración (CI) para un tipo de recurso específico:
>
> - Compruebe que registra AWS Config correctamente la configuración actual del recurso, excluyendo las etiquetas.
> - Compruebe que AWS Config se actualiza la configuración registrada cuando se realiza un cambio en el recurso.

Identificador: REQUIRED_TAGS

Tipos de recursos: AWS::ACM::Certificate AWS::AutoScaling::AutoScalingGroup AWS::CloudFormation::Stack, AWS::CodeBuild::Project, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::SecurityGroup AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup, AWS::Redshift::ClusterSecurityGroup, AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnetGroup AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

tag1Key, Tipo: cadena, Predeterminado: CostCenter

Clave de la etiqueta requerida.

tag1Value (opcional), Tipo: CSV

Valor opcional de la etiqueta requerida. Separe los valores con comas.

tag2Key (opcional), Tipo: cadena

Clave de una segunda etiqueta obligatoria.

tag2Value (opcional), Tipo: CSV

Valor opcional de la segunda etiqueta obligatoria. Separe los valores con comas.

tag3Key (opcional), Tipo: cadena

Clave de una tercera etiqueta obligatoria.

tag3Value (opcional), Tipo: CSV

Valor opcional de la tercera etiqueta obligatoria. Separe los valores con comas.

tag4Key (opcional), Tipo: cadena

Clave de una cuarta etiqueta obligatoria.

tag4Value (opcional), Tipo: CSV

Valor opcional de la cuarta etiqueta obligatoria. Separe los valores con comas.

tag5Key (opcional), Tipo: cadena

Clave de una quinta etiqueta obligatoria.

tag5Value (opcional), Tipo: CSV

Valor opcional de la quinta etiqueta requerida. Separe los valores con comas.

tag6Key (opcional), Tipo: cadena

Clave de una sexta etiqueta obligatoria.

tag6Value (opcional), Tipo: CSV

Valor opcional de la sexta etiqueta obligatoria. Separe los valores con comas.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

restricted-common-ports

> **Important**
>
> Para esta regla, el identificador de la regla (RESTRICTED_INCOMING_TRAFFIC) y el nombre de la regla () son diferentes. restricted-common-ports

Comprueba si los grupos de seguridad que se están utilizando no permiten el tráfico del protocolo de control de transmisión (TCP) entrante sin restricciones a los puertos especificados. La regla es COMPLIANT si:

- El acceso a los puertos está bloqueado para todo el tráfico TCP.

- El acceso a los puertos está abierto al tráfico TCP mediante reglas de entrada, donde el origen es una IPv4 dirección única o un rango de IPv4 direcciones en notación CIDR que no cubre todas las direcciones («0.0.0.0/0"). IPv4
- El acceso a los puertos está abierto al tráfico TCP mediante reglas de entrada, en las que el origen es una IPv6 dirección única o un rango de IPv6 direcciones en notación CIDR que no cubre todas IPv6 las direcciones («:: /0)»).

La regla es NON_COMPLIANT si las direcciones IP de las conexiones TCP entrantes no están restringidas a los puertos especificados.

Identificador: RESTRICTED_INCOMING_TRAFFIC

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de desencadenador: cambios de configuración y periódicos

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

blockedPort1 (opcional), Tipo: int, Predeterminado: 20

Número de puerto TCP bloqueado. El valor predeterminado 20 corresponde a la transferencia de datos del Protocolo de transferencia de archivos (FTP).

blockedPort2 (opcional), Tipo: int, Valor predeterminado: 21

Número de puerto TCP bloqueado. El valor predeterminado 21 corresponde al control de comandos del Protocolo de transferencia de archivos (FTP).

blockedPort3 (opcional), Tipo: int, Valor predeterminado: 3389

Número de puerto TCP bloqueado. El valor predeterminado 3389 corresponde al Protocolo de escritorio remoto (RDP).

blockedPort4 (opcional), Tipo: int, Valor predeterminado: 3306

Número de puerto TCP bloqueado. El valor predeterminado 3306 corresponde al protocolo MySQL.

blockedPort5 (opcional), Tipo: int, Valor predeterminado: 4333

Número de puerto TCP bloqueado. Se utiliza para un puerto específico relevante para su entorno.

blockedPorts (opcional), Tipo: CSV

Lista separada por comas de los números de puerto TCP bloqueados. Por ejemplo, 20, 21, 3306, 3389.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

root-account-hardware-mfa-habilitado

Comprueba si tu AWS cuenta está habilitada para usar un dispositivo de hardware de autenticación multifactor (MFA) para iniciar sesión con credenciales raíz. La regla es NON_COMPLIANT si se permite a cualquier dispositivo MFA iniciar sesión con las credenciales raíz.

> **Note**
>
> No se aplica a cuentas sin credenciales de usuario raíz
> Esta regla devuelve `NOT_APPLICABLE` si las credenciales de usuario raíz no están presentes.
> Reglas administradas y tipos de recursos de IAM globales
> Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar AWS Config en AWS las regiones en las que AWS Config estaban disponibles antes de febrero de 2022. Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.
> Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.
> A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Identificador: ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Centro), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

root-account-mfa-enabled

Comprueba si el usuario raíz de tu AWS cuenta requiere una autenticación multifactor para iniciar sesión en la consola. La regla no es compatible si el usuario de la cuenta raíz de AWS Identity and Access Management (IAM) (IAM) no tiene habilitada la autenticación multifactor (MFA).

> **Note**
>
> No se aplica a cuentas sin credenciales de usuario raíz
> Esta regla devuelve `NOT_APPLICABLE` si las credenciales de usuario raíz no están presentes.
> Reglas administradas y tipos de recursos de IAM globales
> Los tipos de recursos de IAM globales incorporados antes de febrero de 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, y`AWS::IAM::User`) solo se pueden registrar en las regiones AWS Config en AWS las que estaban disponibles antes de febrero de 2022. AWS Config Estos tipos de recursos no se pueden registrar en las regiones admitidas AWS Config después de febrero de 2022. Para ver una lista de esas regiones, consulta AWS Recursos de grabación | Recursos globales.
> Si registra los tipos de recursos de IAM globales en al menos una región, las reglas periódicas que informan del cumplimiento de los tipos de recursos de IAM globales realizarán evaluaciones en todas las regiones en las que se añada la regla periódica, aunque no

haya activado el registro de tipos de recursos de IAM globales en la región en la que se ha añadido la regla periódica.
A fin de evitar evaluaciones innecesarias, solo debería implementar reglas periódicas que informen del cumplimiento en un tipo de recurso de IAM global en una de las regiones compatibles. Para ver una lista de las reglas administradas que se admiten en qué regiones, consulte la lista de reglas AWS Config administradas por disponibilidad regional.

Identificador: ROOT_ACCOUNT_MFA_ENABLED

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Centro), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ruta 53- health-check-tagged

Comprueba si las comprobaciones de estado de Amazon Route 53 tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _HEALTH_CHECK_TAGGED ROUTE53

Tipos de recursos: AWS::Route53::HealthCheck

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ruta 53- hosted-zone-tagged

Comprueba si las zonas alojadas de Amazon Route 53 tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _HOSTED_ZONE_TAGGED ROUTE53

Tipos de recursos: AWS::Route53::HostedZone

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ruta 53- query-logging-enabled

Comprueba si el registro de consultas de DNS está habilitado en una zona alojada pública de Amazon Route 53. La regla es NON_COMPLIANT si el registro de consultas de DNS está habilitado en las zonas alojadas públicas de Amazon Route 53.

Identificador: _QUERY_LOGGING_ENABLED ROUTE53

Tipos de recursos: AWS::Route53::HostedZone

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ruta 53- - etiquetada resolver-firewall-domain-list

Comprueba si las listas de dominios del firewall de Amazon Route 53 Resolver tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _RESOLVER_FIREWALL_DOMAIN_LIST_TAGGED ROUTE53

Tipos de recursos: AWS::Route53Resolver::FirewallDomainList

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS

GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ruta 53- -asociación-etiquetada resolver-firewall-rule-group

Comprueba si las asociaciones de grupos de reglas de firewall de Amazon Route 53 Resolver tienen etiquetas. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: ROUTE53 _RESOLVER_FIREWALL_RULE_GROUP_ASSOCIATION_TAGGED

Tipos de recursos: AWS::Route53Resolver::FirewallRuleGroupAssociation

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ruta 53- - etiquetada resolver-firewall-rule-group

Comprueba si los grupos de reglas de firewall de Amazon Route 53 Resolver tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _RESOLVER_FIREWALL_RULE_GROUP_TAGGED ROUTE53

Tipos de recursos: AWS::Route53Resolver::FirewallRuleGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

ruta 53- resolver-resolver-rule-tagged

Comprueba si las reglas de solucionadores de Amazon Route 53 Resolver tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: _RESOLVER_RESOLVER_RULE_TAGGED ROUTE53

Tipos de recursos: AWS::Route53Resolver::ResolverRule

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rum-app-monitor-cloudwatch-registros habilitados

Comprueba si los monitores de aplicaciones Amazon CloudWatch RUM tienen habilitados CloudWatch los registros. La regla NO ES COMPATIBLE si está configurada. CwLogEnabled es falsa.

Identificador: RUM_APP_MONITOR_CLOUDWATCH_LOGS_ENABLED

Tipos de recursos: AWS::RUM::AppMonitor

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), África (Ciudad del Cabo), Asia Pacífico (Hong Kong), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

rum-app-monitor-tagged

Comprueba si los monitores de aplicaciones Amazon CloudWatch RUM tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: RUM_APP_MONITOR_TAGGED

Tipos de recursos: AWS::RUM::AppMonitor

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), África (Ciudad del Cabo), Asia Pacífico (Hong Kong), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3 express-dir-bucket-lifecycle -reglas-check

Comprueba si hay reglas de ciclo de vida configuradas para un bucket de directorio de Amazon S3 Express. La regla es NON_COMPLIANT si no hay reglas de configuración del ciclo de vida activas o si la configuración no coincide con los valores de los parámetros.

Identificador: S3EXPRESS_DIR_BUCKET_LIFECYCLE_RULES_CHECK

Tipos de recursos: AWS::S3Express::DirectoryBucket

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Asia-Pacífico (Mumbai), Este de EE. UU. (Ohio), Europa (Irlanda), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Tokio) y Oeste de EE. UU. (Oregón)

Parámetros:

targetExpirationDays (Opcional), Tipo: int

Número de días después de la creación tras los cuales se eliminan los objetos de los buckets de directorio de Amazon S3 Express.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

solo access-point-in-vpc s3

Comprueba si un punto de acceso Amazon S3 no permite el acceso desde Internet (NetworkOrigin es VPC). La regla NO CUMPLE CON LAS NORMAS si NetworkOrigin se trata de Internet.

Identificador: S3_ACCESS_POINT_IN_VPC_ONLY

Tipos de recursos: AWS::S3::AccessPoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

bloques s3 access-point-public-access -

Los puntos de acceso de Amazon S3 deben tener habilitada la configuración de bloqueo del acceso público La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.

Identificador: S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

Tipos de recursos: AWS::S3::AccessPoint

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

excludedAccessPoints (Opcional), Tipo: CSV

Lista separada por comas de nombres de puntos de acceso de Amazon S3 públicos permitidos.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

bloques s3 account-level-public-access -

Comprueba si la configuración requerida del bloqueo de acceso público se configura en el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

> **Note**
>
> Si utiliza esta regla, asegúrese de que Bloqueo de acceso público de Amazon S3 esté activado. La regla se activa mediante cambios, por lo que no se invocará a menos que Bloqueo de acceso público de Amazon S3 esté activado. Si Bloqueo de acceso público de Amazon S3 no está activado, la regla devuelve INSUFFICIENT_DATA. Esto significa que es posible que aún tenga algunos buckets públicos. Para obtener más información sobre la configuración de Bloquear el acceso público a su almacenamiento de Amazon S3.

Identifier (Identificador): S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

Tipos de recursos: AWS::S3::AccountPublicAccessBlock

Tipo de desencadenador: cambios de configuración (el estado actual no está comprobado, solo se evalúa cuando los cambios generan nuevos eventos)

> **Note**
>
> Esta regla solo se activa cuando se producen cambios en la configuración de la región específica en la que se encuentra el punto de conexión de S3. En todas las demás regiones, la regla se comprueba periódicamente. Si se ha realizado un cambio en otra región, es posible que se produzca un retraso antes de que la regla devuelva NON_COMPLIANT.

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central),

Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

RestrictPublicBuckets (Opcional), Tipo: cadena, Valor predeterminado: True

RestrictPublicBuckets se aplica o no, el valor predeterminado es True

BlockPublicPolicy (Opcional), Tipo: cadena, Valor predeterminado: True

BlockPublicPolicy se aplica o no, el valor predeterminado es True

BlockPublicAcls (Opcional), Tipo: cadena, Valor predeterminado: True

BlockPublicAcls se aplica o no, el valor predeterminado es True

IgnorePublicAcls (Opcional), Tipo: cadena, Valor predeterminado: True

IgnorePublicAcls se aplica o no, el valor predeterminado es True

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

s3- account-level-public-access -bloques-periódicos

Comprueba si la configuración requerida del bloqueo de acceso público se configura en el nivel de cuenta. La regla es NON_COMPLIANT si el elemento de configuración no coincide con uno o más ajustes de los parámetros (o valores predeterminados).

Identificador: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas las regiones compatibles AWS

Parámetros:

IgnorePublicAcls (Opcional), Tipo: cadena

IgnorePublicAcls se aplica o no, el valor predeterminado es True

BlockPublicPolicy (Opcional), Tipo: cadena

BlockPublicPolicy se aplica o no, el valor predeterminado es True

BlockPublicAcls (Opcional), Tipo: cadena

BlockPublicAcls se aplica o no, el valor predeterminado es True

RestrictPublicBuckets (Opcional), Tipo: cadena

RestrictPublicBuckets se aplica o no, el valor predeterminado es True

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-acl-prohibited

Comprueba si los buckets de Amazon Simple Storage Service (Amazon S3) permiten permisos de usuario a través de listas de control de acceso (). ACLs La regla es NON_COMPLIANT si ACLs está configurada para el acceso de los usuarios en Amazon S3 Buckets.

Identificador: S3_BUCKET_ACL_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-blacklisted-actions-prohibited

Comprueba si una política de bucket de Amazon Simple Storage Service (Amazon S3) no permite acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directores de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna `s3:GetBucket*` acción ni `s3:DeleteObject` en ningún objeto del bucket. La regla es NON_COMPLIANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

> **Note**
>
> La regla solo comprobará las entidades de la propiedad Entidad principal y no tendrá en cuenta las condiciones de la propiedad Condición de una política

Identificador: S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

blacklistedActionPattern, Tipo: CSV

Lista separada por comas de patrones de acción incluidos en la lista negra, por ejemplo, s3: GetBucket * y s3:. DeleteObject

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

habilitado para bucket-cross-region-replication s3

Comprueba si ha activado la replicación entre regiones de S3 para los buckets de Amazon S3. La regla es NON_COMPLIANT si no hay reglas de replicación habilitadas para la replicación entre regiones.

Identificador: S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-default-lock-enabled

Comprueba si el bucket de S3 tiene habilitado el bloqueo de forma predeterminada. La regla es NON_COMPLIANT si el bloqueo no está habilitado.

Identificador: S3_BUCKET_DEFAULT_LOCK_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

mode (opcional), Tipo: cadena

mode: (opcional): parámetro de modo con valores válidos de GOVERNANCE o COMPLIANCE.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-level-public-access -prohibido

Comprueba si los buckets de S3 son de acceso público. La regla es NON_COMPLIANT si un bucket de S3 no aparece en el parámetro `excludedPublicBuckets` y la configuración en el nivel del bucket es pública.

Identificador: S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

excludedPublicBuckets (Opcional), Tipo: CSV

> Lista separada por comas de nombres de buckets de Amazon S3 públicos permitidos y conocidos.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-logging-enabled

Comprueba si el registro está habilitado para los buckets de S3. La regla es NON_COMPLIANT si el registro no está habilitado.

Identificador: S3_BUCKET_LOGGING_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

targetPrefix (opcional), Tipo: cadena

Prefijo del bucket de S3 para almacenar registros de acceso al servidor.

targetBucket (opcional), Tipo: cadena

Bucket de S3 de destino para almacenar registros de acceso al servidor.

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con reglas. AWS Config Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "BucketName": "amzn-s3-demo-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "amzn-s3-demo-destination-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-mfa-delete-enabled

Comprueba si la eliminación de MFA está habilitada en la configuración de control de versiones de bucket de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

Identificador: S3_BUCKET_MFA_DELETE_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

s3- bucket-policy-grantee-check

Comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por alguno de AWS los principales, usuarios federados, principales de servicio, direcciones IP o VPCs que usted proporcione. La regla es COMPLIANT si no está presente una política de bucket.

Por ejemplo, si el parámetro de entrada a la regla es la lista de dos entidades principales: `111122223333` y `444455556666` y la política de bucket especifica que solo `111122223333` puede obtener acceso al bucket, la regla es COMPLIANT. Con los mismos parámetros de entrada: si la política de bucket especifica que `111122223333` y `444455556666` pueden obtener acceso al bucket, también será COMPLIANT.

Sin embargo, si la política de bucket especifica que `999900009999` puede obtener acceso al bucket, la regla es NON_COMPLIANT.

> **Note**
>
> Si una política de bucket contiene más de una instrucción, cada instrucción de la política de buckets se evalúa según esta regla.

Identificador: S3_BUCKET_POLICY_GRANTEE_CHECK

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

awsPrincipals (opcional), Tipo: CSV

Lista de principales separados por comas, como el usuario de IAM ARNs, el rol de IAM y las cuentas. ARNs AWS Debe proporcionar el ARN completo o utilizar una coincidencia parcial. Por ejemplo, «arn:aws:iam: :role/» o «arn:aws:iam: ::role/*». `AccountID` `role_name` `AccountID` Si el valor proporcionado no coincide exactamente con el ARN de la entidad principal especificado en la política del bucket, la regla es NON_COMPLIANT.

servicePrincipals (opcional), Tipo: CSV

Lista separada por comas de las entidades principales de servicio, por ejemplo, cloudtrail.amazonaws.com, lambda.amazonaws.com.

federatedUsers (opcional), Tipo: CSV

Lista separada por comas de los proveedores de identidades para la federación de identidades web, tales como los proveedores de identidad Amazon Cognito y SAML. Por ejemplo, cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider.

ipAddresses (opcional), Tipo: CSV

Lista separada por comas de direcciones IP con formato CIDR, por ejemplo, 10.0.0.1, 192.168.1.0/24, 2001:db8::/32.

vpcIds (opcional), Tipo: CSV

Lista separada por comas de Amazon Virtual Private Clouds (Amazon VPC), por ejemplo, «vpc-1234abc0 IDs, vpc-ab1234c0".

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-policy-not-more -permisivo

Comprueba que las políticas del bucket de Amazon Simple Storage Service no otorguen otros permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que proporcione.

> **Note**
>
> Si proporciona un valor de parámetro no válido, verá el siguiente mensaje de error: Value for controlPolicy parameter must be an Amazon S3 bucket policy.

Identificador: S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

controlPolicy, Tipo: cadena

Política del bucket de Amazon S3 que define un límite superior en los permisos de sus buckets de S3. La política puede tener una longitud máxima de 1024 caracteres.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-public-read-prohibited

Comprueba si sus buckets de Amazon S3 no permiten acceso de lectura público. La regla comprueba la configuración de Block Public Access, la política del bucket y la lista de control de acceso (ACL) del bucket.

La regla se cumple cuando se dan las dos condiciones siguientes:

- La configuración de Block Public Access restringe las políticas públicas o la política del bucket no permite el acceso de lectura público.
- La configuración Bloquear el acceso público restringe el acceso público ACLs o la ACL del bucket no permite el acceso de lectura público.

La regla no se cumple en los siguientes casos:

- Si la configuración Bloquear el acceso público no restringe las políticas públicas, AWS Config evalúa si la política permite el acceso de lectura público. Si la política permite el acceso de lectura público, la regla no se cumple.
- Si la configuración Bloquear el acceso público no restringe el depósito público ACLs, AWS Config evalúa si la ACL del depósito permite el acceso de lectura público. Si la ACL del bucket permite acceso de lectura público, la regla no se cumple.

> **Note**
>
> Para que se considere no pública, una política de bucket de S3 debe conceder acceso solo a valores fijos. Esto significa valores que no contienen un comodín ni el siguiente elemento de política de IAM: Variables.

Identificador: S3_BUCKET_PUBLIC_READ_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de desencadenador: cambios de configuración y periódicos

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-public-write-prohibited

Comprueba si sus buckets de Amazon S3 no permiten acceso de escritura público. La regla comprueba la configuración de Block Public Access, la política del bucket y la lista de control de acceso (ACL) del bucket.

La regla se cumple cuando se dan las dos condiciones siguientes:

- La configuración de Block Public Access restringe las políticas públicas o la política del bucket no permite el acceso de escritura público.
- La configuración Bloquear el acceso público restringe el acceso público ACLs o la ACL del bucket no permite el acceso de escritura público.

La regla no se cumple en los siguientes casos:

- Si la configuración Bloquear el acceso público no restringe las políticas públicas, AWS Config evalúa si la política permite el acceso de escritura público. Si la política permite el acceso de escritura público, la regla no se cumple.
- Si la configuración Bloquear el acceso público no restringe el segmento público ACLs, AWS Config evalúa si la ACL del segmento permite el acceso de escritura público. Si la ACL del bucket permite el acceso de escritura público, la regla no se cumple.

> **Note**
>
> Esta regla no evalúa los cambios en el acceso a bloques públicos en el nivel de cuenta. Para comprobar si los ajustes de bloqueo de acceso público necesarios están configurados a nivel de cuenta, consulte s3- account-level-public-access -blocks y s3- account-level-public-access -blocks-periodic.

> **Note**
>
> Para que se considere no pública, una política de bucket de S3 debe conceder acceso solo a valores fijos. Esto significa valores que no contienen un comodín ni el siguiente elemento de política de IAM: Variables.

Identificador: S3_BUCKET_PUBLIC_WRITE_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de desencadenador: cambios de configuración y periódicos

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-replication-enabled

Comprueba si los buckets de S3 tienen habilitadas las reglas de replicación. La regla es NON_COMPLIANT si un bucket de S3 no tiene una regla de replicación o tiene una regla de replicación que no está habilitada.

Identificador: S3_BUCKET_REPLICATION_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

ReplicationType (Opcional), Tipo: cadena

Valores aceptados: CROSS-REGION SAME-REGION. Introduzca CROSS-REGION como regla para comprobar que todos los buckets solo tengan habilitada la replicación entre regiones. Introduzca SAME-REGION como regla para comprobar que todos los buckets solo tengan habilitada la replicación en la misma región.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

habilitado para bucket-server-side-encryption s3

Comprueba que su bucket de Amazon S3 tenga el cifrado predeterminado de Amazon S3 habilitado o que la política de bucket de Amazon S3 deniegue explícitamente las solicitudes de `put-object` sin cifrado del lado del servidor mediante AES-256 o AWS Key Management Service. La regla es NON_COMPLIANT si el bucket de Amazon S3 no está cifrado de forma predeterminada.

Identificador: S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-ssl-requests-only

Comprueba si los buckets de S3 tienen políticas que requieran que las solicitudes utilicen SSL/TLS. La regla es NON_COMPLIANT si algún bucket de S3 tiene políticas que permitan solicitudes HTTP.

Identificador: S3_BUCKET_SSL_REQUESTS_ONLY

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

s3-bucket-tagged

Comprueba si los buckets de Amazon S3 tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: S3_BUCKET_TAGGED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- bucket-versioning-enabled

Comprueba si el control de versiones está habilitado para los buckets de S3. Opcionalmente, la regla comprueba si la eliminación de MFA está habilitada para los buckets de S3.

Identificador: S3_BUCKET_VERSIONING_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

isMfaDeleteActivado (opcional), Tipo: cadena

La eliminación de MFA está habilitada para los buckets de S3.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- default-encryption-kms

Comprueba si los buckets de S3 están cifrados con el Servicio de administración de AWS claves (AWS KMS). La regla no cumple con los requisitos si el bucket de S3 no está cifrado con una AWS clave KMS.

Identificador: S3_DEFAULT_ENCRYPTION_KMS

Tipos de recursos:, AWS::S3::Bucket AWS::KMS::Key

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

Lista separada por comas de claves de AWS KMS ARNs permitidas para cifrar buckets de Amazon S3.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

s3- event-notifications-enabled

Comprueba si las notificaciones de eventos de Amazon S3 están habilitadas en un bucket de S3. La regla es NON_COMPLIANT si las notificaciones de eventos de S3 no están configuradas en un bucket o si el tipo de evento o destino no coinciden con los parámetros `eventTypes` destinationArn.

Identificador: S3_EVENT_NOTIFICATIONS_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

destinationArn (opcional), Tipo: cadena

El nombre del recurso de Amazon (ARN) del destino de la notificación del evento (tema de Amazon SNS, AWS Lambda, Amazon SQS Queue).

eventTypes (opcional), Tipo: CSV

Lista separada por comas de los tipos de eventos de Amazon S3 preferidos

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- last-backup-recovery-point -creado

Comprueba si se ha creado un punto de recuperación para Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si el bucket de Amazon S3 no tiene ningún punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: S3_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Amazon EBS para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

El nombre del bucket de Amazon S3 para que la regla lo compruebe.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- lifecycle-policy-check

Comprueba si se ha configurado una regla de ciclo de vida para un bucket de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si no hay reglas de configuración del ciclo de vida activas o si la configuración no coincide con los valores de los parámetros.

Identificador: S3_LIFECYCLE_POLICY_CHECK

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

targetTransitionDays (Opcional), Tipo: int

Número de días después de crear los objetos cuando estos pasan a una clase de almacenamiento específico (por ejemplo, 30 días).

targetExpirationDays (Opcional), Tipo: int

Número de días después de crear los objetos cuando estos se eliminan (por ejemplo, 395 días).

targetTransitionStorageClase (opcional), Tipo: cadena

Tipo de clase de almacenamiento de destino Por ejemplo, Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Para obtener más información, consulte Descripción y administración de clases de almacenamiento de Amazon S3.

targetPrefix (opcional), Tipo: cadena

Prefijo de objeto de Amazon S3 para identificar uno o más objetos.

bucketNames (opcional), Tipo: CSV

Lista separada por comas de los nombres de los buckets de Amazon S3 que tienen habilitada la política de ciclo de vida.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- meets-restore-time-target

Comprueba si el tiempo de restauración de los buckets de Amazon Simple Storage Service (Amazon S3) se ajusta a la duración especificada. La regla es NON_COMPLIANT si un bucket LatestRestoreExecutionTimeMinutes de Amazon S3 es superior maxRestoreTime a minutos.

Identificador: S3_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

maxRestoreTime, Tipo: int

Valor numérico del tiempo de ejecución de restauración máximo permitido.

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Amazon EBS para que la regla las compruebe, en formato JSON .

resourceId (opcional), Tipo: cadena

El nombre del bucket de Amazon S3 para que la regla lo compruebe.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

s3- resources-in-logically-air -bóveda con huecos

Comprueba si los buckets de Amazon Simple Storage Service (Amazon S3) están dentro de un almacén aislado lógicamente. La regla es NON_COMPLIANT si hay un bucket de Amazon S3 que no está en un almacén aislado lógicamente dentro del período de tiempo especificado.

Identificador: S3_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: periódico

Región de AWS: solo está disponible en las regiones Europa (Estocolmo), Medio Oriente (Baréin), Asia-Pacífico (Mumbai), Europa (París), Este de EE. UU. (Ohio), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Asia-Pacífico (Osaka), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Oeste de EE. UU. (Norte de California), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Amazon EBS para que la regla las compruebe, en formato JSON .

resourceId (opcional), Tipo: cadena

El nombre del bucket de Amazon S3 para que la regla lo compruebe.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 2184 horas y 91 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

plano resources-protected-by-backup s3

Verifica si los buckets de Amazon Simple Storage Service (Amazon S3) están protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el bucket de Amazon S3 no está cubierto por un plan de copia de seguridad.

Identificador: S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los buckets de Amazon S3 para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

El nombre del bucket de Amazon S3 para que la regla lo compruebe.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

s3- version-lifecycle-policy-check

Comprueba si los buckets habilitados para la versión de Amazon Simple Storage Service (Amazon S3) tienen configurada la política de ciclo de vida. La regla es NON_COMPLIANT si la política de ciclo de vida de Amazon S3 no está habilitada.

Identificador: S3_VERSION_LIFECYCLE_POLICY_CHECK

Tipos de recursos: AWS::S3::Bucket

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

bucketNames (opcional), Tipo: CSV

> Lista separada por comas de los nombres de los buckets de Amazon S3 que tienen habilitada la política de ciclo de vida.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

sagemaker-app-image-config-etiquetado

Comprueba si las configuraciones de imagen de las SageMaker aplicaciones de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: SAGEMAKER_APP_IMAGE_CONFIG_TAGGED

Tipos de recursos: AWS::SageMaker::AppImageConfig

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), China (Ningxia), Región Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

sagemaker-domain-in-vpc

Comprueba si un SageMaker dominio de Amazon utiliza una Amazon Virtual Private Cloud (VPC) propiedad del cliente para el tráfico que no es de EFS. La regla no cumple con las normas si está configurada. AppNetworkAccessType no está establecida en. VpcOnly

Identificador: SAGEMAKER_DOMAIN_IN_VPC

Tipos de recursos: AWS::SageMaker::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sagemaker-domain-tagged

Comprueba si SageMaker los dominios de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: SAGEMAKER_DOMAIN_TAGGED

Tipos de recursos: AWS::SageMaker::Domain

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sagemaker-endpoint-configuration-kms-configurado por clave

Comprueba si la AWS clave del Servicio de administración de claves (AWS KMS) está configurada para una configuración de SageMaker punto final de Amazon. La regla es NON_COMPLIANT si no se especifica KmsKeyId " para la configuración del SageMaker punto de conexión de Amazon.

Identifier (Identificador): SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

Tipos de recursos: AWS::SageMaker::EndpointConfig

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

kmsKeyArns (Opcional), Tipo: cadena

> Lista separada por comas de claves de AWS KMS específicas ARNs permitidas para una configuración de SageMaker punto final de Amazon.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

sagemaker-endpoint-config-prod-recuento de instancias

Comprueba si las configuraciones de los SageMaker puntos de conexión de Amazon tienen variantes de producción InitialInstanceCount `` establecidas en un valor superior a 1. La regla no cumple con los requisitos si la variante de producción `InitialInstanceCount` es igual a 1.

Identificador: SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUNT

Tipos de recursos: AWS::SageMaker::EndpointConfig

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sagemaker-feature-group-tagged

Comprueba si los grupos de SageMaker funciones de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: SAGEMAKER_FEATURE_GROUP_TAGGED

Tipos de recursos: AWS::SageMaker::FeatureGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), China (Ningxia), Región Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sagemaker-image-description

Comprueba si SageMaker las imágenes de Amazon tienen una descripción. La regla no cumple con las normas si está configurada. ImageDescription no existe.

Identificador: SAGEMAKER_IMAGE_DESCRIPTION

Tipos de recursos: AWS::SageMaker::Image

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), China (Ningxia), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sagemaker-image-tagged

Comprueba si SageMaker las imágenes de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: SAGEMAKER_IMAGE_TAGGED

Tipos de recursos: AWS::SageMaker::Image

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), China (Ningxia), Región Europa (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

sagemaker-model-in-vpc

Comprueba si un SageMaker modelo de Amazon utiliza una Amazon Virtual Private Cloud (Amazon VPC) para el tráfico de contenedores. La regla NO ES COMPATIBLE si está configurada. VpcConfig no existe.

Identificador: SAGEMAKER_MODEL_IN_VPC

Tipos de recursos: AWS::SageMaker::Model

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sagemaker-model-isolation-enabled

Comprueba si un SageMaker modelo de Amazon tiene activado el aislamiento de red. La regla NO CUMPLE CON LOS REQUISITOS si está configurada. EnableNetworkIsolation es falsa.

Identificador: SAGEMAKER_MODEL_ISOLATION_ENABLED

Tipos de recursos: AWS::SageMaker::Model

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sagemaker-notebook-instance-inside-PVC

Comprueba si una instancia de Amazon SageMaker Notebook se lanza dentro de una VPC o dentro de una lista de subredes aprobadas. La regla es NON_COMPLIANT si una instancia de cuaderno no se lanza dentro de una VPC o si su ID de subred no está incluido en la lista de parámetros.

Identificador: SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

Tipos de recursos: AWS::SageMaker::NotebookInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich) AWS GovCloud

Parámetros:

SubnetIds (Opcional), Tipo: CSV

> Lista de subredes separadas por comas en las IDs que se pueden lanzar las instancias de notebook.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

sagemaker-notebook-instance-kms-configurado por clave

Comprueba si hay una AWS clave del Servicio de administración de claves (AWS KMS) configurada para una instancia de Amazon SageMaker Notebook. La regla no es compatible si no se especifica 'KmsKeyId' para la instancia de SageMaker bloc de notas.

Identifier (Identificador): SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

Tipos de recursos: AWS::SageMaker::NotebookInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

kmsKeyArns (Opcional), Tipo: cadena

> Lista separada por comas de claves AWS KMS ARNs permitidas para una instancia de Amazon SageMaker Notebook.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sagemaker-notebook-instance-platform-versión

Comprueba si una instancia de Sagemaker Notebook está configurada para usar una versión de identificador de plataforma compatible. La regla es NON_COMPLIANT si una instancia de Notebook no utiliza la versión de identificador de plataforma compatible especificada, como se indica en el parámetro.

Identificador: SAGEMAKER_NOTEBOOK_INSTANCE_PLATFORM_VERSION

Tipos de recursos: AWS::SageMaker::NotebookInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

supportedPlatformIdentifierVersiones, Tipo: CSV

> Lista separada por comas de la versión de identificador de plataforma compatible para que la regla la compruebe.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sagemaker-notebook-instance-root-control de acceso

Comprueba si la SageMaker RootAccess configuración de Amazon está habilitada para las instancias de Amazon SageMaker Notebook. La regla no es compatible si el RootAccess ajuste está establecido en «Activado» para una instancia de Amazon SageMaker Notebook.

Identificador: SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

Tipos de recursos: AWS::SageMaker::NotebookInstance

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

sagemaker-notebook-no-direct-acceso a internet

Comprueba si el acceso directo a Internet está deshabilitado para una instancia de Amazon SageMaker Notebook. La regla no cumple con los requisitos si una instancia de SageMaker notebook tiene acceso a Internet.

Identifier (Identificador): SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

Tipos de recursos: AWS::SageMaker::NotebookInstance

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

secretsmanager-rotation-enabled-check

Comprueba si el secreto de AWS Secrets Manager tiene habilitada la rotación. La regla también comprueba un parámetro opcional de `maximumAllowedRotationFrequency`. Si se especifica el parámetro, la frecuencia de rotación del secreto se compara con la frecuencia máxima permitida. La regla es NON_COMPLITY si el secreto no está programado para la rotación. La regla tampoco cumple con los requisitos si la frecuencia de rotación es superior al número especificado en el parámetro maximumAllowedRotation Frecuencia.

> **Note**
>
> Volver a evaluar esta regla en un plazo de 4 horas tras la primera evaluación no tendrá ningún efecto en los resultados.

Identificador: SECRETSMANAGER_ROTATION_ENABLED_CHECK

Tipos de recursos: AWS::SecretsManager::Secret

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

maximumAllowedRotationFrequencyInHours (Opcional), Tipo: int

Frecuencia máxima de rotación permitida del secreto en horas.

maximumAllowedRotationFrecuencia (opcional), Tipo: int

Frecuencia máxima de rotación permitida del secreto en días.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

secretsmanager-scheduled-rotation-success-comprobar

Comprueba si AWS los secretos de Secrets Manager se han rotado correctamente según el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.

> **Note**
>
> Retrasos en el registro
> Los resultados de la evaluación de esta regla se pueden retrasar hasta 2 días a partir de la fecha de rotación no cumplida. Para una supervisión más inmediata, consulte Supervisar AWS Secrets Manager con Amazon CloudWatch en la Guía del usuario de Secrets Manager.
> Secretos sin rotación
> La regla devuelve `NOT_APPLICABLE` para secretos que no están configurados para rotación.

Identificador: SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

Tipos de recursos: AWS::SecretsManager::Secret

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

secretsmanager-secret-periodic-rotation

Comprueba si AWS los secretos de Secrets Manager se han rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.

Identificador: SECRETSMANAGER_SECRET_PERIODIC_ROTATION

Tipos de recursos: AWS::SecretsManager::Secret

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

maxDaysSinceRotación (opcional), Tipo: int

Número máximo de días durante el que un secreto puede permanecer sin cambios. El valor predeterminado es 90 días.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

secretsmanager-secret-unused

Comprueba si se AWS ha accedido a los secretos de Secrets Manager en un número específico de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número 'unusedForDays' de días. El valor predeterminado es 90 días.

Contexto: se recomienda eliminar de forma rutinaria los secretos no utilizados. Los antiguos usuarios pueden abusar de los secretos no utilizados, ya que no necesitan acceder a ellos. Además, a medida que más usuarios acceden a un secreto, es cada vez más probable que alguien lo utilice de forma incorrecta o haya permitido el acceso a una entidad no autorizada. Eliminar los secretos no utilizados ayuda a revocar el acceso secreto a los usuarios que ya no lo necesitan y puede reducir el costo de usar AWS Secrets Manager.

Identificador: SECRETSMANAGER_SECRET_UNUSED

Tipos de recursos: AWS::SecretsManager::Secret

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

unusedForDays (Opcional), Tipo: int

Número de días durante el que un secreto puede permanecer sin cambios. El valor predeterminado es 90 días.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

secretsmanager-using-cmk

Comprueba si todos los secretos AWS Secrets Manager están cifrados con Clave administrada de AWS (`aws/secretsmanager`) o con una clave gestionada por el cliente que se creó en AWS Key Management Service (AWS KMS). La regla es COMPLIANT si un secreto se cifra usando una clave administrada por el cliente. Esta regla es NON_COMPLIANT si un secreto se cifra mediante `aws/secretsmanager`.

> **Note**
>
> Esta regla no tiene acceso a las claves administradas por los clientes de varias cuentas y evalúa los secretos como NON_COMPLIANT cuando se utiliza una clave de varias cuentas.

Identificador: SECRETSMANAGER_USING_CMK

Tipos de recursos: AWS::SecretsManager::Secret

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

kmsKeyArns (Opcional), Tipo: CSV

Lista separada por comas de Amazon Resource Names (ARNs) de claves de KMS para comprobar si las claves se utilizan en el cifrado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

securityhub-enabled

Comprueba si AWS Security Hub está activado para una AWS cuenta. La regla es NON_COMPLIANT si AWS Security Hub no está activado.

Identificador: SECURITYHUB_ENABLED

Tipo de disparador: periódico

Región de AWS: Todas las regiones compatibles AWS

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

security-account-information-provided

Comprueba si has proporcionado información de contacto de seguridad para los contactos de tu AWS cuenta. La regla es NON_COMPLIANT si no se proporciona la información de contacto de seguridad de la cuenta.

Identificador: SECURITY_ACCOUNT_INFORMATION_PROVIDED

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

service-catalog-portfolio-tagged

Comprueba si los recursos de la cartera de AWS Service Catalog tienen etiquetas. También se pueden especificar las claves de etiqueta necesarias. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: SERVICE_CATALOG_PORTFOLIO_TAGGED

Tipos de recursos: AWS::ServiceCatalog::Portfolio

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

service-catalog-shared-within-organización

Comprueba si AWS Service Catalog comparte carteras con una organización (un conjunto de AWS cuentas tratadas como una sola unidad) cuando la integración está habilitada con AWS Organizations. La regla es NON_COMPLIANT si el valor de Tipo al compartir es ACCOUNT.

Identifier: SERVICE_CATALOG_SHARED_WITHIN_ORGANIZATION

Tipos de recursos: AWS::ServiceCatalog::Portfolio

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

service-vpc-endpoint-enabled

Comprueba si el punto de conexión de servicio para el servicio proporcionado en el parámetro de regla se ha creado para cada Amazon Virtual Private Cloud (Amazon VPC). La regla es NON_COMPLIANT si una Amazon VPC no tiene ningún punto de conexión de VPC creado para el servicio.

Identifier (Identificador): SERVICE_VPC_ENDPOINT_ENABLED

Tipos de recursos: AWS::EC2::VPC

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

serviceName, Tipo: cadena

Nombre corto o sufijo del servicio. Nota: Para obtener una lista de los nombres de servicios disponibles o una lista de sufijos válidos, utilice DescribeVpcEndpointServices.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ses-malware-scanning-enabled

Comprueba si el análisis de malware y spam de los mensajes entrantes está activado para Amazon Simple Email Service (Amazon SES). La regla es NON_COMPLIANT si el análisis de malware y spam no está activado.

Identificador: SES_MALWARE_SCANNING_ENABLED

Tipos de recursos: AWS::SES::ReceiptRule

Tipo de disparador: periódico

Región de AWS: solo está disponible en las regiones de Europa (Irlanda), Este de EE. UU. (Norte de Virginia) y Oeste de EE. UU. (Oregón)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ses-sending-tls-required

Comprueba si el conjunto de configuraciones de Amazon Simple Email Service (SES) tiene el cifrado TLS aplicado para la entrega del correo electrónico. La regla no cumple con los requisitos si la política de TLS no está establecida como «REQUERIR» en el conjunto de configuraciones.

Identificador: SES_SENDING_TLS_REQUIRED

Tipos de recursos: AWS::SES::ConfigurationSet

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hong Kong), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

shield-advanced-enabled-autorenew

Comprueba si AWS Shield Advanced está activado en su AWS cuenta y si esta suscripción está configurada para renovarse automáticamente. La regla es COMPLIANT si Shield Avanzado y la renovación automática están habilitadas.

> **Note**
>
> El punto de enlace de la API solo AWS Shield Advanced está disponible en la región EE.UU. Este (Norte de Virginia). Esta regla solo debería programarse para ejecutarse en la región Este de EE. UU. (Norte de Virginia).

Identificador: SHIELD_ADVANCED_ENABLED_AUTORENEW

Tipo de disparador: periódico

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

shield-drt-access

Comprueba si el Shield Response Team (SRT) puede acceder a tu AWS cuenta. La regla no cumple con las normas si AWS Shield Advanced está habilitada, pero la función de acceso a la SRT no está configurada.

Identifier (Identificador): SHIELD_DRT_ACCESS

Tipo de disparador: periódico

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sns-encrypted-kms

Comprueba si los temas de SNS están cifrados con el Servicio de administración de AWS claves (AWS KMS). La regla no es compatible si un tema de SNS no está cifrado con KMS. AWS Si lo desea, especifique la clave ARNs, el alias ARNs, el nombre del alias o la clave de la regla que IDs desee comprobar.

Identificador: SNS_ENCRYPTED_KMS

Tipos de recursos: AWS::SNS::Topic

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

kmsKeyIds (Opcional), Tipo: CSV

Lista separada por comas de los AWS nombres de recursos de Amazon (ARNs) clave de KMS, alias de KMS ARNs, nombres de alias de KMS o clave de KMS IDs para comprobar la regla.

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con AWS Config reglas. Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sns-topic-message-delivery-habilitado para notificaciones

Comprueba si el registro de Amazon Simple Notification Service (SNS) está habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

Identificador: SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

Tipos de recursos: AWS::SNS::Topic

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Europa (Zúrich)) Región

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sns-topic-no-public-acceso

Comprueba si la política de acceso a los temas de Amazon SNS permite el acceso público. Si la política de acceso del tema de SNS permite el acceso público, la regla es NON_COMPLIANT.

> **Note**
>
> Para que se considere no pública, una política de SNS debe conceder acceso solo a valores fijos. Esto significa valores que no contienen un comodín ni el siguiente elemento de política de IAM: Variables.

Identificador: SNS_TOPIC_NO_PUBLIC_ACCESS

Tipos de recursos: AWS::SNS::Topic

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sqs-queue-dlq-check

Comprueba si las colas de Amazon Simple Queue Service (Amazon SQS) están configuradas para usar colas de mensajes fallidos (DLQ). Esta regla es NON_COMPLIANT si una cola de Amazon SQS no tiene ninguna configuración para usar DLQ.

Identificador: SQS_QUEUE_DLQ_CHECK

Tipos de recursos: AWS::SQS::Queue

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

sqs-queue-no-public-acceso

Comprueba si la política de acceso a colas SQS permite el acceso público. La regla es NON_COMPLIANT si la política de acceso a colas SQS permite el acceso público.

> **Note**
>
> Para que se considere no pública, una política de SQS debe conceder acceso solo a valores fijos. Esto significa valores que no contienen un comodín ni el siguiente elemento de política de IAM: Variables.

Identificador: SQS_QUEUE_NO_PUBLIC_ACCESS

Tipos de recursos: AWS::SQS::Queue

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México AWS GovCloud (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región Europa (España), Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

sqs-queue-policy-full-control de acceso

Comprueba si la política de acceso a colas SQS permite el acceso completo. La regla es NON_COMPLIANT si la política de SQS contiene “SQS:*” dentro de “Action” y “Effect” es “Allow”.

Permitir: SQS_QUEUE_POLICY_FULL_ACCESS_CHECK

Tipos de recursos: AWS::SQS::Queue

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla de plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ssm-automation-block-public-compartir

Comprueba si AWS Systems Manager Documents tiene activado el bloqueo para compartir en público. La regla es NON_COMPLIANT si Documentos de Systems Manager tiene deshabilitado el bloqueo de uso compartido público.

Identificador: SSM_AUTOMATION_BLOCK_PUBLIC_SHARING

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ssm-automation-logging-enabled

Comprueba si AWS Systems Manager Automation tiene activado el CloudWatch registro de Amazon. La regla devuelve NON_COMPLIANT si Systems Manager Automation no tiene habilitado el CloudWatch registro.

Identificador: SSM_AUTOMATION_LOGGING_ENABLED

Tipos de recurso: AWS::::Account

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central) y Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ssm-document-not-public

Comprueba si AWS los documentos de Systems Manager propiedad de la cuenta son públicos. La regla es NON_COMPLIANT si los documentos de Systems Manager con el propietario Self son públicos.

Identificador: SSM_DOCUMENT_NOT_PUBLIC

Tipos de recursos: AWS::SSM::Document

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles, excepto la región de Asia Pacífico (Taipéi)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

ssm-document-tagged

Comprueba si AWS los documentos de Systems Manager tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de

etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: SSM_DOCUMENT_TAGGED

Tipos de recursos: AWS::SSM::Document

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

stepfunctions-state-machine-tagged

Comprueba si las máquinas de estado de AWS Step Functions tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: STEPFUNCTIONS_STATE_MACHINE_TAGGED

Tipos de recursos: AWS::StepFunctions::StateMachine

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

step-functions-state-machine-habilitado para el registro

Comprueba si la máquina AWS Step Functions tiene activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

Identificador: STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

Tipos de recursos: AWS::StepFunctions::StateMachine

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

cloudWatchLogGroupArns (Opcional), Tipo: CSV

> Lista de nombres de recursos de Amazon (ARNs) separados por comas para los grupos de CloudWatch registros de Amazon Logs. La regla comprueba si los grupos de registros especificados están configurados para los registros de su máquina de estado.

logLevel (opcional), Tipo: cadena

Nivel de registro mínimo para su máquina de estado. Los valores válidos son: ALL, ERROR y FATAL.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

storagegateway-last-backup-recovery-punto creado

Comprueba si se creó un punto de recuperación para los volúmenes AWS de Storage Gateway. La regla es NON_COMPLIANT si el volumen de Storage Gateway no tiene un punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::StorageGateway::Volume

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Storage Gateway para que la regla las compruebe, en formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: cadena

ID del volumen de Storage Gateway que debe comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

storagegateway-resources-in-logically-air-gapped-vault

Comprueba si los volúmenes AWS de Storage Gateway están en un almacén cerrado de forma lógica. La regla no cumple con los requisitos si un volumen de AWS Storage Gateway no se encuentra en un almacén con huecos lógicos dentro del período de tiempo especificado.

Identificador: STORAGEGATEWAY_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Tipos de recursos: AWS::StorageGateway::Volume

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Región China (Ningxia) AWS GovCloud

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Storage Gateway para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID del volumen de Storage Gateway que debe comprobar la regla.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 2184 horas y 91 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

storagegateway-resources-protected-by-plan de respaldo

Comprueba si los volúmenes AWS de Storage Gateway están protegidos por un plan de backup. La regla es NON_COMPLIANT si el volumen de Storage Gateway no está cubierto por un plan de copia de seguridad.

Identificador: STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::StorageGateway::Volume

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia) Región

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de los volúmenes de Storage Gateway para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID del volumen de Storage Gateway que debe comprobar la regla.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

subnet-auto-assign-public-ip deshabilitada

Comprueba si las subredes de Amazon Virtual Private Cloud (Amazon VPC) están configuradas para asignar automáticamente direcciones IP públicas a las instancias lanzadas en ellas. Esta regla es COMPATIBLE si las subredes no asignan automáticamente direcciones públicas IPv4 o IPv6 direcciones. Esta regla no cumple con las normas si las subredes asignan automáticamente direcciones o públicas. IPv4 IPv6

> **Warning**
>
> Esta regla no distingue entre rangos de direcciones de unidifusión globales (GUA) privados y públicos y tratará todos los IPv6 rangos GUA como infracciones cuando la asignación automática esté habilitada.

Identificador: SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

Tipos de recursos: AWS::EC2::Subnet

Tipo de disparador: cambios de configuración

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

Ninguno

Evaluación proactiva

Para ver los pasos sobre cómo ejecutar esta regla en modo proactivo, consulte Cómo evaluar sus recursos con AWS Config reglas. Para que esta regla devuelva COMPLIANT en modo proactivo, el esquema de configuración de recursos de la StartResourceEvaluationAPI debe incluir las siguientes entradas, codificadas como una cadena:

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

Para obtener más información sobre la evaluación proactiva, consulte Modo de evaluación.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

transfer-agreement-description

Comprueba si los acuerdos AWS Transfer Family tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe.

Identificador: TRANSFER_AGREEMENT_DESCRIPTION

Tipos de recursos: AWS::Transfer::Agreement

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Europa (Región Zurich (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation Plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

transfer-agreement-tagged

Comprueba si los acuerdos de AWS Transfer Family tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: TRANSFER_AGREEMENT_TAGGED

Tipos de recursos: AWS::Transfer::Agreement

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), China (Ningxia), Europa (Región (Zúrich)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

transfer-certificate-description

Comprueba si los certificados AWS Transfer Family tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe.

Identificador: TRANSFER_CERTIFICATE_DESCRIPTION

Tipos de recursos: AWS::Transfer::Certificate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

transfer-certificate-tagged

Comprueba si los certificados AWS Transfer Family tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: TRANSFER_CERTIFICATE_TAGGED

Tipos de recursos: AWS::Transfer::Certificate

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

transfer-connector-logging-enabled

Comprueba si AWS Transfer Family Connector publica registros en Amazon CloudWatch. La regla no cumple con los requisitos si un Connector no tiene un LoggingRole asignado.

Identificador: TRANSFER_CONNECTOR_LOGGING_ENABLED

Tipos de recursos: AWS::Transfer::Connector

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), Asia Pacífico (Tailandia), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

transfer-connector-tagged

Comprueba si los conectores AWS Transfer Family tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: TRANSFER_CONNECTOR_TAGGED

Tipos de recursos: AWS::Transfer::Connector

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

transfer-family-server-no-ftp

Comprueba si un servidor creado con AWS Transfer Family utiliza FTP para la conexión de punto final. La regla es NON_COMPLIANT si el protocolo del servidor para la conexión del punto de conexión está habilitado para FTP.

Identificador: TRANSFER_FAMILY_SERVER_NO_FTP

Tipos de recursos: AWS::Transfer::Server

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi), Canadá Oeste (Calgary) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

transfer-profile-tagged

Comprueba si los perfiles de AWS Transfer Family tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: TRANSFER_PROFILE_TAGGED

Tipos de recursos: AWS::Transfer::Profile

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

transfer-workflow-description

Comprueba si los flujos de trabajo de AWS Transfer Family tienen una descripción. La regla es NON_COMPLIANT si configuration.Description no existe o es una cadena vacía.

Identificador: TRANSFER_WORKFLOW_DESCRIPTION

Tipos de recursos: AWS::Transfer::Workflow

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

transfer-workflow-tagged

Comprueba si los flujos de trabajo de AWS Transfer Family tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: TRANSFER_WORKFLOW_TAGGED

Tipos de recursos: AWS::Transfer::Workflow

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia) AWS GovCloud

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de

etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

virtualmachine-last-backup-recovery-punto creado

Comprueba si se creó un punto de recuperación para AWS VirtualMachines Backup-Gateway. La regla no es compatible si una AWS puerta de enlace de respaldo VirtualMachines no tiene un punto de recuperación correspondiente creado dentro del período de tiempo especificado.

Identificador: VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::BackupGateway::VirtualMachine

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de AWS Backup-Gateway VirtualMachines para que la regla las compruebe, en formato JSON. `{"tagkey" : "tagValue"}`

resourceId (opcional), Tipo: cadena

ID de AWS Backup-Gateway VirtualMachine para que la regla lo compruebe.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 744 horas y 31 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

virtualmachine-resources-in-logically-air-gapped-vault

Comprueba si AWS Backup-Gateway VirtualMachines se encuentra en una bóveda aislada de forma lógica. La regla no es compatible si una AWS puerta de enlace de respaldo no VirtualMachines se encuentra en un almacén con huecos lógicos dentro del período de tiempo especificado.

Identificador: VIRTUALMACHINE_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Tipos de recursos: AWS::BackupGateway::VirtualMachine

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas de AWS Backup-Gateway VirtualMachines para que la regla las compruebe, en formato JSON.

resourceId (opcional), Tipo: cadena

ID de AWS Backup-Gateway VirtualMachine para que la regla lo compruebe.

recoveryPointAgeValor (opcional), Tipo: int, Valor predeterminado: 1

Valor numérico de la edad máxima permitida. No más de 2184 horas y 91 días.

recoveryPointAgeUnidad (opcional), Tipo: cadena, Valor predeterminado: days

Unidad de tiempo para la edad máxima permitida. Valores aceptados: hours y days

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

virtualmachine-resources-protected-by-plan de respaldo

Comprueba si AWS Backup-Gateway VirtualMachines está protegido por un plan de respaldo. La regla no cumple con los requisitos si el Backup-Gateway no VirtualMachine está cubierto por un plan de respaldo.

Identificador: VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::BackupGateway::VirtualMachine

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), China (Ningxia), Región Europa (Zúrich)

Parámetros:

resourceTags (opcional), Tipo: cadena

Etiquetas para AWS Backup-Gateway VirtualMachines para que la regla las compruebe, en formato JSON. `{"tagkey" : "tagValue"}`

resourceId (opcional), Tipo: cadena

ID de AWS Backup-Gateway VirtualMachine para que la regla lo compruebe.

crossRegionList (Opcional), Tipo: cadena

Lista separada por comas de las regiones de destino para conservar la copia de seguridad entre regiones.

crossAccountList (Opcional), Tipo: cadena

Lista separada por comas de las cuentas de destino para conservar una copia de seguridad entre cuentas

maxRetentionDays (Opcional), Tipo: int

Período máximo de retención en días para Bloqueo de almacenes de AWS Backup.

minRetentionDays (Opcional), Tipo: int

Período mínimo de retención en días para Bloqueo de almacenes de AWS Backup.

backupVaultLockMarcar (opcional), Tipo: cadena

Valores aceptados: True o False. Introduzca True para la regla para comprobar si el recurso está guardado en un almacén bloqueado.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

vpc-default-security-group-cerrado

Comprueba que el grupo de seguridad predeterminado de cualquier Amazon Virtual Private Cloud (Amazon VPC) no permita tráfico entrante o saliente. La regla es NON_COMPLIANT si el grupo de seguridad predeterminado tiene reglas de tráfico entrante o saliente.

> **Note**
>
> Puede haber un retraso entre el AWS Config registro y la eliminación de los recursos relacionados, como los grupos de seguridad predeterminados, que se eliminan como parte de la eliminación de Amazon VPC. En consecuencia, aunque se hayan eliminado o corregido todos los grupos de seguridad predeterminados u otros recursos relacionados, la regla puede mostrar NON_COMPLIANT hasta el siguiente proceso de referencia de la cuenta.

Identificador: VPC_DEFAULT_SECURITY_GROUP_CLOSED

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de disparador: cambios de configuración

Región de AWS: Solo disponible en las regiones Oriente Medio (Baréin), EE.UU. Este (Ohio), Europa (Irlanda), Europa (Fráncfort), EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

vpc-endpoint-enabled

Comprueba si todos los servicios especificados en el parámetro tienen un punto de conexión de Amazon VPC. La regla es NON_COMPLIANT si hay una Amazon VPC que no tenga ningún punto de conexión de VPC creado para cada servicio especificado. Si lo desea, puede especificar algunos elementos VPCs para que la regla los compruebe.

Identificador: VPC_ENDPOINT_ENABLED

Tipos de recursos: AWS::EC2::VPC

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Osaka), Asia Pacífico (Malasia), México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

serviceNames, Tipo: CSV

Lista separada por comas de los nombres de servicios o puntos de conexión. Ejemplo: “access-analyzer, appconfig, cloudtrail” o “com.amazonaws.region.access-analyzer”. Úselo DescribeVpcEndpointServices para los nombres disponibles.

vpcIds (opcional), Tipo: CSV

Lista separada por comas de Amazon VPC IDs para puntos de enlace de VPC. Si se proporciona, la regla es NON_COMPLIANT si los servicios especificados en el parámetro serviceName no tienen uno de estos puntos de conexión de VPC.

scopeConfigResourceTipos (opcional), Tipo: CSV

Lista de tipos de recursos de AWS Config separados por comas para que la regla los compruebe. Si se especifica, la regla devuelve un estado de cumplimiento solo si al menos un recurso especificado está registrado en la cuenta. Por ejemplo: "»AWS::SNS::Topic.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

vpc-flow-logs-enabled

Comprueba si los registros de flujo de Amazon Virtual Private Cloud (Amazon VPC) se encuentran y están habilitados para todos los Amazon. VPCs La regla es NON_COMPLIANT si los registros de flujo no están habilitados para al menos una VPC de Amazon.

Identificador: VPC_FLOW_LOGS_ENABLED

Tipos de recursos: AWS::EC2::VPC

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

trafficType (opcional), Tipo: cadena

TrafficType de registros de flujo

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

vpc-network-acl-unused-comprobar

Comprueba si hay listas de control de acceso a la red (red ACLs) sin utilizar. La regla es COMPLIANT si cada ACL de red está asociada a una subred. La regla es NON_COMPLIANT si una ACL de red no está asociada a una subred.

Identificador: VPC_NETWORK_ACL_UNUSED_CHECK

Tipos de recursos: AWS::EC2::NetworkAcl

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia) AWS GovCloud , (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

vpc-peering-dns-resolution-comprobar

Comprueba si la resolución de DNS desde la accepter/requester VPC a la IP privada está habilitada. La regla no es compatible si la resolución de DNS desde la accepter/requester VPC a la IP privada no está habilitada.

Identificador: VPC_PEERING_DNS_RESOLUTION_CHECK

Tipos de recursos: AWS::EC2::VPCPeeringConnection

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

vpcIds (opcional), Tipo: CSV

Lista separada por comas de VPC IDs que se deben comprobar.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

vpc-sg-open-only-to-authorized-ports

Comprueba si los grupos de seguridad que permiten el tráfico entrante sin restricciones (0.0.0.0/0 o ::/0) solo permiten conexiones TCP o UDP entrantes en los puertos autorizados. La regla es NON_COMPLIANT si dichos grupos de seguridad no tienen puertos especificados en los parámetros de la regla.

> **Note**
>
> Esta regla evalúa los grupos de EC2 seguridad de Amazon con la regla de entrada establecida en IPv4 ='0.0.0.0/0' o =': :/'. IPv6 Si el grupo de seguridad no tiene uno de esos destinos, esta regla devuelve `NOT_APPLICABLE`.

Identificador: VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de desencadenador: cambios de configuración y periódicos

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

authorizedTcpPorts (Opcional), Tipo: cadena

Lista separada por comas de los puertos TCP autorizados a estar abiertos para 0.0.0.0/0 o ::/0. Los intervalos se definen con un guion, por ejemplo, "443,1020-1025".

authorizedUdpPorts (Opcional), Tipo: cadena

Lista separada por comas de los puertos UDP autorizados a estar abiertos para 0.0.0.0/0 o ::/0.. Los intervalos se definen con un guion, por ejemplo, "500,1020-1025".

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

vpc-sg-port-restriction-comprobar

Comprueba si los grupos de seguridad limitan el tráfico entrante a los puertos restringidos de forma explícita desde 0.0.0.0/0 o ::/0. La regla no cumple con los requisitos si los grupos de seguridad permiten el tráfico entrante desde el 0.0.0.0/0 o: :/0 a través de los puertos 22/3389 o según se especifique en los parámetros. TCP/UDP

Identificador: VPC_SG_PORT_RESTRICTION_CHECK

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de disparador: periódico

Región de AWS: Todas AWS las regiones compatibles, excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Malasia), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary)

Parámetros:

restrictPorts (opcional), Tipo: CSV

Lista separada por comas de puertos que no deberían estar abiertos para el tráfico entrante en todo el rango de IP. Rango de números de puerto válidos, entre 0 y 65535. Si no se especifica nada, la regla comprueba de forma predeterminada el 22 y el 3389.

protocolType (opcional), Tipo: cadena

El tipo de protocolo de transmisión que debe comprobar la regla. Algunos valores válidos son TCP, UDP y ALL (no distingue mayúsculas y minúsculas). Si se pone en ALL, la regla comprobará si hay reglas que utilicen alguno de estos protocolos (TCP, UDP o ALL (-1)). El valor predeterminado es ALL.

excludeExternalSecurityGrupos (opcional), Tipo: booleano

Indicador booleano para excluir la evaluación de los grupos de seguridad externos. Si se pone en “true”, la regla no incluirá los grupos de seguridad externos en la evaluación. De lo contrario, con el valor en “false”, se evaluarán todos los grupos de seguridad. El valor predeterminado es “true”.

ipType (opcional), Tipo: cadena

La versión del protocolo de Internet (IP) para que la regla la compruebe. Los valores válidos incluyen 'IPv4', 'yIPv6' ALL '(no distingue entre mayúsculas y minúsculas). Si no se especifica nada, la regla comprueba de forma predeterminada ALL.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

vpc-vpn-2-tunnels-up

Comprueba si los dos túneles de red privada virtual (VPN) proporcionados por la AWS Site-to-Site VPN están en estado ACTIVO. La regla es NON_COMPLIANT si uno o ambos túneles tienen el estado DOWN.

Identificador: VPC_VPN_2_TUNNELS_UP

Tipos de recursos: AWS::EC2::VPNConnection

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Oriente Medio (Baréin), China (Pekín), Asia Pacífico (Osaka), Israel (Tel Aviv) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

wafv2-logging-enabled

Comprueba si el registro está habilitado en AWS WAFv2 las listas de control de acceso web (web ACLs) regionales y globales. La regla es NON_COMPLIANT si el registro está activado pero el destino del registro no coincide con el valor del parámetro.

> **Note**
>
> Excepción para Amazon Security Lake
> Esta regla no comprueba el registro realizado con Security Lake para la AWS WAFV2 web ACLs.

Identificador: WAFV2 _LOGGING_ENABLED

Tipos de recursos: AWS::WAFv2::WebACL

Tipo de disparador: periódico

Región de AWS: Todas las AWS regiones compatibles

Parámetros:

KinesisFirehoseDeliveryStreamArns (Opcional), Tipo: CSV

Lista separada por comas del flujo de entrega de Kinesis Firehose ARNs

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guerra 2- rulegroup-logging-enabled

Comprueba si la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas está habilitada. La regla no cumple con los requisitos si el valor '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.

Contexto: AWS WAFV2 (Web Application Firewall, versión 2), le permite crear AWS WAF reglas para proteger sus aplicaciones web de las vulnerabilidades y vulnerabilidades más comunes de la web. Un grupo de AWS WAF reglas es un conjunto de AWS WAF reglas que puede asociar a una ACL (lista de control de acceso) web para definir el comportamiento deseado para el tráfico de sus aplicaciones web. Para obtener más información, consulte Uso de reglas de AWS WAF y Uso de reglas de AWS WAF, en la Guía del desarrollador de AWS WAF .

Al configurar la recopilación de métricas de CloudWatch seguridad en un grupo de AWS WAFV2 reglas, puede supervisar las métricas de seguridad, como los ataques de denegación de servicio

distribuida (DDoS) exitosos o fallidos, la inyección de SQL y los ataques de secuencias de comandos entre sitios (XSS). Las métricas de seguridad recopiladas pueden ayudarle a simplificar la investigación.

> **Note**
>
> Si no hay AWS WAF reglas en el grupo de reglas que la AWS WAFV2 regla gestionada deba comprobar, la regla AWS Config AWS Config gestionada vuelve a aparecer. `NOT_APPLICABLE`

Identificador: WAFV2 _RULEGROUP_LOGGING_ENABLED

Tipos de recursos: AWS::WAFv2::RuleGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

guerra 2- rulegroup-not-empty

Comprueba si los grupos de WAFv2 reglas contienen reglas. La regla no es compatible si no hay reglas en un WAFv2 grupo de reglas.

Identificador: _RULEGROUP_NOT_EMPTY WAFV2

Tipos de recursos: AWS::WAFv2::RuleGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), Asia Pacífico (Melbourne), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

guerra 2- webacl-not-empty

Comprueba si una ACL WAFv2 web contiene reglas de WAF o grupos de reglas de WAF. Esta regla NON_COMPLIANT si una ACL web no contiene reglas de WAF ni grupos de reglas de WAF.

Identificador: _WEBACL_NOT_EMPTY WAFV2

Tipos de recursos: AWS::WAFv2::WebACL

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste) AWS GovCloud , México (Central), Asia Pacífico (Taipéi), Canadá oeste (Calgary), Europa (España), Región Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

waf-classic-logging-enabled

Comprueba si el registro está activado en las listas de control AWS de acceso web globales (web ACLs) clásicas de WAF. La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.

Identificador: WAF_CLASSIC_LOGGING_ENABLED

Tipos de recursos: AWS::WAF::WebACL

Tipo de disparador: periódico

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

KinesisFirehoseDeliveryStreamArns (Opcional), Tipo: CSV

> Lista separada por comas del ARN de transmisión de Amazon Kinesis para los registros de WAF. AWS

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

waf-global-rulegroup-not-vacío

Comprueba si un grupo de reglas AWS del WAF Classic contiene alguna regla. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.

Identificador: WAF_GLOBAL_RULEGROUP_NOT_EMPTY

Tipos de recursos: AWS::WAF::RuleGroup

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

waf-global-rule-not-vacío

Comprueba si una regla global AWS de WAF contiene alguna condición. La regla es NON_COMPLIANT si no hay condiciones presentes en la regla global de WAF.

Identificador: WAF_GLOBAL_RULE_NOT_EMPTY

Tipos de recursos: AWS::WAF::Rule

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

waf-global-webacl-not-vacío

Comprueba si una ACL web de WAF Global contiene reglas o grupos de reglas de WAF. Esta regla es NON_COMPLIANT si una ACL web no contiene reglas ni grupos de reglas de WAF.

Identificador: WAF_GLOBAL_WEBACL_NOT_EMPTY

Tipos de recursos: AWS::WAF::WebACL

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en la región Este de EE. UU. (Norte de Virginia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

waf-regional-rulegroup-not-vacío

Comprueba si los grupos de reglas de WAF contienen reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas de WAF.

Identificador: WAF_REGIONAL_RULEGROUP_NOT_EMPTY

Tipos de recursos: AWS::WAFRegional::RuleGroup

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles excepto China (Pekín), Asia Pacífico (Tailandia), Asia Pacífico (Yakarta), Oriente Medio (Emiratos Árabes Unidos), Asia Pacífico (Hyderabad), Asia Pacífico (Osaka), Asia Pacífico (Malasia), (EEUU-Este) AWS GovCloud , (EEUU-Oeste) AWS GovCloud , México (Central), Israel (Tel Aviv), Asia Pacífico (Taipéi), Canadá Oeste (Calgary), Europa (España España), China (Ningxia), Región de Europa (Zúrich)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulteCreación de reglas AWS Config administradas con AWS CloudFormation plantillas.

waf-regional-rule-not-vacío

Comprueba si la regla regional de WAF contiene condiciones. Esta regla es COMPLIANT si la regla regional contiene al menos una condición; de lo contrario es NON_COMPLIANT.

Identificador: WAF_REGIONAL_RULE_NOT_EMPTY

Tipos de recursos: AWS::WAFRegional::Rule

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

waf-regional-webacl-not-vacío

Comprueba si una ACL web regional de WAF contiene reglas o grupos de reglas de WAF. La regla es NON_COMPLIANT si no hay reglas ni grupos de reglas de WAF dentro de una ACL web.

Identificador: WAF_REGIONAL_WEBACL_NOT_EMPTY

Tipos de recursos: AWS::WAFRegional::WebACL

Tipo de disparador: cambios de configuración

Región de AWS: Todas AWS las regiones compatibles, excepto Asia Pacífico (Tailandia), Asia Pacífico (Malasia), (EE. UU. Este) AWS GovCloud , (EE. UU. Oeste), México (Central), Asia Pacífico (Taipéi) y Canadá Oeste (Calgary) AWS GovCloud

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

workspaces-connection-alias-tagged

Comprueba si los alias de WorkSpaces conexión de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: WORKSPACES_CONNECTION_ALIAS_TAGGED

Tipos de recursos: AWS::WorkSpaces::ConnectionAlias

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte[Creación de reglas AWS Config administradas con AWS CloudFormation plantillas](#).

workspaces-root-volume-encryption-habilitado

Comprueba si un WorkSpace volumen de Amazon tiene habilitada la configuración de cifrado del volumen raíz. La regla es NON_COMPLIANT si el cifrado no se ha habilitado para el volumen raíz.

Identificador: WORKSPACES_ROOT_VOLUME_ENCRYPTION_ENABLED

Tipos de recursos: AWS::WorkSpaces::Workspace

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), África (Ciudad del Cabo), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney), Canadá (centro) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

workspaces-user-volume-encryption-habilitado

Comprueba si un WorkSpace volumen de Amazon tiene habilitada la configuración de cifrado de volúmenes de usuarios. La regla es NON_COMPLIANT si el cifrado no se ha habilitado para el volumen de usuario.

Identificador: WORKSPACES_USER_VOLUME_ENCRYPTION_ENABLED

Tipos de recursos: AWS::WorkSpaces::Workspace

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), África (Ciudad del Cabo), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney), Canadá (centro) y China (Ningxia)

Parámetros:

Ninguno

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

workspaces-workspace-tagged

Comprueba si los WorkSpaces espacios de trabajo de Amazon tienen etiquetas. También puede especificar claves de etiqueta. La regla es NON_COMPLIANT si no hay etiquetas o si las claves de etiqueta especificadas no están presentes. La regla no comprueba si las etiquetas comienzan por “aws:”.

Identificador: WORKSPACES_WORKSPACE_TAGGED

Tipos de recursos: AWS::WorkSpaces::Workspace

Tipo de disparador: cambios de configuración

Región de AWS: solo está disponible en las regiones Asia-Pacífico (Mumbai), África (Ciudad del Cabo), Europa (Irlanda), Europa (Fráncfort), América del Sur (São Paulo), Este de EE. UU. (Norte de Virginia), Asia-Pacífico (Seúl), Europa (Londres), Asia-Pacífico (Tokio), Oeste de EE. UU. (Oregón), Asia-Pacífico (Singapur), Asia-Pacífico (Sídney) y Canadá (centro)

Parámetros:

requiredKeyTags (Opcional), Tipo: CSV

> Lista separada por comas de claves de etiqueta que la regla debe comprobar. Si se proporciona, la regla es NON_COMPLIANT si el recurso evaluado no contiene estas claves. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. No se permiten las claves de etiqueta que comiencen por “aws:”.

AWS CloudFormation plantilla

Para crear reglas AWS Config administradas con AWS CloudFormation plantillas, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.

Lista de reglas AWS Config administradas por modo de evaluación

AWS Config actualmente admite las siguientes reglas administradas. Antes de usar estas reglas, consulte Consideraciones.

Evaluación proactiva

Las reglas proactivas son reglas que respaldan el modo de evaluación proactiva de los recursos que no se han implementado todavía. Esto le permite evaluar si un conjunto de propiedades de un

recurso, si se utiliza para definir un AWS recurso, cumpliría o no lo es, dado el conjunto de reglas proactivas que tiene en su cuenta de su región. Para obtener más información, consulte Modos de evaluación.

> **Note**
>
> Las reglas proactivas no corrigen los recursos que están marcados como NON_COMPLIANT ni impiden su implementación.

Evaluación proactiva

- eip-attached

Evaluación de detectives

Las reglas de detectives son reglas que admiten el modo de evaluación de detectives para los recursos que ya se han implementado. Esto le permite evaluar los ajustes de configuración de los recursos existentes.

> **Note**
>
> Actualmente, todas las AWS Config reglas respaldan la evaluación policial.

Evaluación de detectives

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-desactivado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado

- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío

- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc

- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-en reposo
- appsync-cache-ct-encryption-en tránsito
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo

- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check

- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configurado
- cloudfront-distribution-key-group-habilitado
- cloudfront-no-deprecated-ssl-protocolos
- cloudfront-origin-access-identity-habilitado
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-habilitado para oac
- cloudfront-s3- origin-access-control-enabled
- cloudfront-s3- origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encriptado
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged

- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito

- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled

- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest
- ec2-stopped-instance

- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo

- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged

- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar

- iam-saml-provider-tagged
- iam-server-certificate-expiration-comprobar
- iam-server-certificate-tagged
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-no-policies-comprobar
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged

- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged

- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted

- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable

- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito

- rds-sql-server-logs-a Cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- health-check-tagged
- ruta 53- hosted-zone-tagged
- ruta 53- query-logging-enabled

- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3 -rules-check express-dir-bucket-lifecycle
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado

- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- ses-sending-tls-required
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged

- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-default-security-group-cerrado
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-vacío
- waf-global-rule-not-vacío
- waf-global-webacl-not-vacío
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Lista de reglas AWS Config administradas por tipo de activador

AWS Config actualmente admite las siguientes reglas administradas. Antes de usar estas reglas, consulte Consideraciones.

Cambios de configuración

Las reglas activadas por cambios son reglas que se AWS Config evalúan en respuesta a los cambios de configuración.

Cambios de configuración

- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado

- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check

- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-authorization-check
- appsync-cache-ct-encryption-en reposo
- appsync-cache-ct-encryption-en tránsito
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo

- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check

- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configurado
- cloudfront-distribution-key-group-habilitado
- cloudfront-no-deprecated-ssl-protocolos
- cloudfront-origin-access-identity-habilitado
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-habilitado para oac
- cloudfront-s3- origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encriptado
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-settings-check
- cloudwatch-metric-stream-tagged
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización

- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado

- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibido
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ebs-snapshot-block-public-acceso
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached

- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -eni security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled

- ec2- vpn-connection-tagged
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled

- eks-cluster-oldest-supported-versión
- eks-cluster-supported-version
- eks-fargate-profile-tagged
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-verificación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description

- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- iam-customer-policy-blocked-kms-acciones
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-oidc-provider-tagged
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-saml-provider-tagged
- iam-server-certificate-tagged
- iam-user-group-membership-comprobar
- iam-user-no-policies-comprobar

- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-stream-backup-retention-comprobar

- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-tagged
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check

- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- required-tags
- ruta 53- health-check-tagged
- ruta 53- hosted-zone-tagged
- ruta 53- query-logging-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3 -rules-check express-dir-bucket-lifecycle
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled

- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- lifecycle-policy-check
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-control de acceso
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-using-cmk
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones

- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- subnet-auto-assign-public-ip-deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-cerrado
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-vpn-2-tunnels-up
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-global-rulegroup-not-vacío
- waf-global-rule-not-vacío
- waf-global-webacl-not-vacío
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Periódico

Las reglas periódicas son reglas que se AWS Config evalúan periódicamente con la frecuencia que usted especifique; por ejemplo, cada 24 horas.

Periódico

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-desactivado
- alb-http-to-https-verificación de redireccionamiento
- api-gwv2- authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-descansar
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- cloudfront-s3- origin-non-existent-bucket
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- dms-replication-not-public
- docdb-cluster-encrypted-in-tránsito
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-public-restorable-comprobar
- ec2- -todos client-vpn-not-authorize
- ec2- ebs-encryption-by-default
- ec2- -creado last-backup-recovery-point
- ec2- meets-restore-time-target
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan

- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ecr-private-image-scanning-habilitado
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eks-cluster-logging-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-acceso
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2- acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- event-data-store-cmk-habilitado para el cifrado
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-habilitado
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-comprobar
- iam-server-certificate-expiration-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled

- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- kinesis-firehose-delivery-stream-encriptado
- kms-cmk-not-scheduled-para su eliminación
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-automatic-minor-version-habilitado para la actualización
- mq-cloudwatch-audit-logging-habilitado
- mq-no-public-access
- multi-region-cloud-trail-habilitado
- netfw-logging-enabled
- nlb-logging-enabled
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-mysql-instance-encrypted-en tránsito
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-sqlserver-encrypted-in-tránsito
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público

- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- s3- -bloques-periódicos account-level-public-access
- s3- -creado last-backup-recovery-point
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-punto creado

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-port-restriction-comprobar
- wafv2-logging-enabled
- waf-classic-logging-enabled

Híbrido

Las reglas híbridas son reglas que se AWS Config evalúan tanto en respuesta a los cambios de configuración como de forma periódica.

Híbrido

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-comprobar
- ec2- -ami instance-launched-with-allowed
- incoming-ssh-disabled
- no-unrestricted-route-to-igw
- restricted-incoming-traffic
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

Lista de reglas AWS Config administradas por región y disponibilidad

AWS Config actualmente admite las siguientes reglas administradas. Antes de usar estas reglas, consulte Consideraciones.

Región del este de EE. UU. (Ohio)

Este de EE. UU. (Ohio)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado

- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists

- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo

- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado

- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured

- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault

- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check

- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled

- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az

- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- frauddetector-entity-type-tagged
- frauddetector-label-tagged

- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones

- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación

- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos

- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado

- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3 -rules-check express-dir-bucket-lifecycle
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access

- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave

- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-default-security-group-cerrado
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región Este de EE. UU. (Norte de Virginia)

Este de EE. UU. (Norte de Virginia)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged

- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description

- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-en reposo
- appsync-cache-ct-encryption-en tránsito
- appsync-cache-encryption-at-descanso

- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configurado
- cloudfront-distribution-key-group-habilitado
- cloudfront-no-deprecated-ssl-protocolos
- cloudfront-origin-access-identity-habilitado
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-habilitado para oac
- cloudfront-s3- origin-access-control-enabled
- cloudfront-s3- origin-non-existent-bucket
- cloudfront-security-policy-check

- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encriptado
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado

- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required

- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged

- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado

- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe

- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-saml-provider-tagged
- iam-server-certificate-expiration-comprobar
- iam-server-certificate-tagged
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-no-policies-comprobar
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado

- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encriptado

- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado

- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged

- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar

- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check

- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- health-check-tagged
- ruta 53- hosted-zone-tagged
- ruta 53- query-logging-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3 -rules-check express-dir-bucket-lifecycle
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited

- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-default-security-group-cerrado
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-vacío
- waf-global-rule-not-vacío
- waf-global-webacl-not-vacío
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región del oeste de EE. UU. (Norte de California)

Oeste de EE. UU. (Norte de California)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged

- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged

- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descansar
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description

- athena-workgroup-description
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged

- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check

- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached

- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit

- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo

- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar

- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-comprobar
- macie-auto-sensitive-data-descubrimiento-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización

- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-a Cloudwatch
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged

- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso

- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región del Oeste de EE. UU (Oregón)

Oeste de EE. UU. (Oregón)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado

- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar

- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado

- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled

- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled

- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted

- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check

- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest

- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto

- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar

- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar

- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description

- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola

- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado

- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-a Cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3 -rules-check express-dir-bucket-lifecycle

- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso

- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-default-security-group-cerrado
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports

- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región África (Ciudad del Cabo)

África (Ciudad del Cabo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled

- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description

- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo

- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check

- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización

- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro

- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled

- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description

- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged

- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones

- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- macie-auto-sensitive-data-descubrimiento-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted

- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable

- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-a Cloudwatch
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled

- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo

- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado

- workspaces-workspace-tagged

Región de Asia-Pacífico (Hong Kong)

Asia-Pacífico (Hong Kong)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured

- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on

- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descansar
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite

- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso

- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted

- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled

- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description

- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check

- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo

- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar

- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled

- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp

- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- macie-auto-sensitive-data-descubrimiento-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado

- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl

- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-no-acceso público
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled

- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región de Asia Pacífico (Hyderabad)

Asia-Pacífico (Hyderabad)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento

- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática

- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check

- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas

- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo

- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2-stopped-instance

- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-verificación de cifrado
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión

- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-habilitado
- iam-password-policy
- iam-root-access-key-comprobar
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-comprobar
- mariadb-publish-logs-to-cloudwatch-logs
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-habilitado para el registro
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged

- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado

- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled

- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región Asia-Pacífico (Yakarta)

Asia-Pacífico (Yakarta)

- access-keys-rotated
- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm

- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-enforce-workgroup-configuración

- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- clb-desync-mode-check

- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https

- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged

- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled

- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible

- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-verificación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el equilibrio

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión

- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado

- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar

- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-no-acceso público
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- rum-app-monitor-cloudwatch-habilitado para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access

- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-no-public-acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description

- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región de Asia-Pacífico (Malasia)

Asia-Pacífico (Malasia)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-verificación de redireccionamiento
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra

- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launch-config-public-ip deshabilitado
- beanstalk-enhanced-health-reporting-habilitado
- cloudformation-stack-drift-detection-comprobar
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- cw-loggroup-retention-period-comprobar
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-efs-cifrado activado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-acceso

- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kms-cmk-not-scheduled-para su eliminación
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- multi-region-cloud-trail-habilitado
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled

- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-blacklisted-actions-prohibited
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3- bucket-versioning-enabled

- s3- default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip deshabilitado
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Región de Asia-Pacífico (Melbourne)

Asia-Pacífico (Melbourne)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description

- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- approved-amis-by-id
- approved-amis-by-tag
- appsync-graphql-api-xray-habilitado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed

- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -etiquetado transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado

- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged

- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fms-shield-resource-policy-comprobar

- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-deployment-type-comprobar
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-habilitado
- iam-password-policy
- iam-root-access-key-comprobar
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-solo

- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-habilitado para el registro
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support

- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- resolver-resolver-rule-tagged

- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- plan s3 resources-protected-by-backup -
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-recuento de instancias

- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-acceso
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región de Asia-Pacífico (Mumbai)

Asia-Pacífico (Mumbai)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description

- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged

- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada

- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached

- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip

- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description

- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe

- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged

- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar

- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado

- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled

- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3 -rules-check express-dir-bucket-lifecycle
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado

- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled

- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región Asia-Pacífico (Osaka)

Asia-Pacífico (Osaka)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento

- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descansar
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-envvar-awscred-comprobar

- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-tagged
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged

- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description

- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -etiquetado transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar

- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- macie-auto-sensitive-data-descubrimiento-comprobación
- macie-status-check

- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar

- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled

- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región de Asia-Pacífico (Seúl)

Asia-Pacífico (Seúl)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado

- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check

- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descansar
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check

- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check

- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public

- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log

- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair

- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled

- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled

- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled

- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar

- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled

- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan

- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado

- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled

- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión

- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description

- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región de Asia-Pacífico (Singapur)

Asia-Pacífico (Singapur)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed

- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls

- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración

- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged

- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar

- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https

- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled

- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume

- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc

- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description

- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description

- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado

- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc

- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check

- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito

- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3

- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp

- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región de Asia-Pacífico (Sídney)

Asia-Pacífico (Sídney)

- access-keys-rotated
- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado

- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check

- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado

- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged

- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted

- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged

- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado

- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe

- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged

- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description

- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito

- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público

- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only

- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región de Asia-Pacífico (Taipéi)

Asia-Pacífico (Taipéi)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-verificación de redireccionamiento
- approved-amis-by-id

- approved-amis-by-tag
- cloudformation-stack-drift-detection-comprobar
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- cw-loggroup-retention-period-comprobar
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-comprobar
- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- -ami instance-launched-with-allowed
- ec2- instance-profile-attached
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check

- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-acceso
- eks-secrets-encrypted
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-comprobar
- emr-kerberos-enabled
- emr-master-no-public-ip
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- multi-region-cloud-trail-habilitado
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-in-backup-plan
- rds-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-blacklisted-actions-prohibited

- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3- default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- subnet-auto-assign-public-ip deshabilitado
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Región de Asia-Pacífico (Tailandia)

Asia-Pacífico (Tailandia)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-verificación de redireccionamiento
- apigatewayv2-stage-description
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-execution-logging-habilitado
- api-gw-ssl-enabled

- approved-amis-by-id
- approved-amis-by-tag
- cloudformation-stack-drift-detection-comprobar
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- cw-loggroup-retention-period-comprobar
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-comprobar
- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-profile-attached

- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-acceso
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-habilitado
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-para su eliminación
- lambda-dlq-check

- lambda-function-description
- lambda-function-public-access-prohibido
- multi-region-cloud-trail-habilitado
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-in-backup-plan
- rds-logging-enabled
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-blacklisted-actions-prohibited
- s3- bucket-level-public-access -prohibido
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3- default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip deshabilitado
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Región de Asia-Pacífico (Tokio)

Asia-Pacífico (Tokio)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables

- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento

- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado

- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado

- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default

- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan

- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root

- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado

- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged

- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged

- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled

- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged

- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs

- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado

- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled

- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3 -rules-check express-dir-bucket-lifecycle
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access

- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias

- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty

- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región de Canadá (centro)

Canadá (centro)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitada para la eliminación
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description

- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged

- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descansar
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-enforce-workgroup-configuración

- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged

- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar

- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled

- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged

- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged

- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado

- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad

- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged

- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado

- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio

- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado

- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled

- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged

- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Oeste de Canadá (Calgary)

Oeste de Canadá (Calgary)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- alb-http-drop-invalid-habilitado para encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged

- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- aurora-mysql-cluster-audit-registro
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launch-config-public-ip deshabilitado
- batch-scheduling-policy-tagged
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- cw-loggroup-retention-period-comprobar

- datasync-task-data-verification-habilitado
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted

- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- prefix-list-tagged
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -etiquetado transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-tagged
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-encrypted-check
- efs-file-system-tagged
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-acceso
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- glb-tagged
- glue-ml-transform-tagged
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kms-cmk-not-scheduled-para su eliminación
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-logs
- multi-region-cloud-trail-habilitado

- netfw-subnet-change-protection-habilitado
- nlb-internal-scheme-check
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-habilitado para la actualización
- rds-cluster-deletion-protection-habilitado
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar

- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-blacklisted-actions-prohibited
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- subnet-auto-assign-public-ip deshabilitado
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Región China (Pekín)

China (Pekín)

- access-keys-rotated
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-verificación de redireccionamiento
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-execution-logging-habilitado
- api-gw-ssl-enabled
- approved-amis-by-id

- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-registro
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudfront-s3- origin-non-existent-bucket
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación

- cmk-backing-key-rotation-habilitado
- codebuild-project-environment-privileged-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-report-group-encrypted-en reposo
- cognito-identity-pool-unauth-control de acceso
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-task-logging-enabled
- dax-encryption-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-targetdb-registro
- docdb-cluster-encrypted-in-tránsito
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-deletion-protection-habilitado
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-imdsv2-check
- ec2- -ami instance-launched-with-allowed

- ec2- instance-managed-by-ssm
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- paravirtual-instance-check
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-secrets-encrypted
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para autenticación
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-comprobar
- elb-predefined-security-policy-ssl-comprobar
- emr-kerberos-enabled
- emr-master-no-public-ip
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar

- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-deployment-type-comprobar
- fsx-windows-deployment-type-comprobar
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-spark-job-supported-versión
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-acciones
- iam-inline-policy-blocked-kms-acciones
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- lambda-function-public-access-prohibido
- lambda-function-xray-enabled
- lambda-vpc-multi-az-comprobar
- mfa-enabled-for-iam-acceso a la consola
- mq-active-deployment-mode
- mq-auto-minor-version-habilitado para la actualización

- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- netfw-subnet-change-protection-habilitado
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-enhanced-monitoring-enabled
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-instance-encrypted-en tránsito
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar

- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-routes-dentro de un vpc
- required-tags
- restricted-incoming-traffic
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- lifecycle-policy-check
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet

- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-topic-message-delivery-habilitado para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-habilitado para el registro
- subnet-auto-assign-public-ip-deshabilitado
- transfer-connector-logging-enabled
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- webacl-not-empty
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región China (Ningxia)

China (Ningxia)

- access-keys-rotated

- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-verificación de redireccionamiento
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-execution-logging-habilitado
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-registro
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging

- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-environment-privileged-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-report-group-encrypted-en reposo
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-task-logging-enabled
- dax-encryption-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar

- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-deletion-protection-habilitado
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-imdsv2-check
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -eni security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecs-capacity-provider-termination-comprobar

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-secrets-encrypted
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para autenticación
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-comprobar
- emr-kerberos-enabled
- emr-master-no-public-ip
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-deployment-type-comprobar
- fsx-windows-deployment-type-comprobar
- glue-job-logging-enabled
- glue-spark-job-supported-versión
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-acciones
- iam-inline-policy-blocked-kms-acciones
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- instances-in-vpc

- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- mfa-enabled-for-iam-acceso a la consola
- mq-active-deployment-mode
- mq-auto-minor-version-habilitado para la actualización
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- netfw-subnet-change-protection-habilitado
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-descansar

- rds-enhanced-monitoring-enabled
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-routes-dentro de un vpc
- required-tags
- restricted-incoming-traffic
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited

- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- lifecycle-policy-check
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-topic-message-delivery-habilitado para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check

- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-habilitado para el registro
- subnet-auto-assign-public-ip-deshabilitado
- transfer-connector-logging-enabled
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- webacl-not-empty
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado

Región de Europa (Fráncfort)

Europa (Fráncfort)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id

- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-en reposo
- appsync-cache-ct-encryption-en tránsito
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check

- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización

- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo

- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted

- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado

- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault

- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado

- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar

- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado

- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged

- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia

- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito

- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled

- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización

- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-plan de respaldo
- vpc-default-security-group-cerrado
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región de Europa (Irlanda)

Europa (Irlanda)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc

- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check

- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged

- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public

- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log

- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair

- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad

- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged

- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-habilitado
- ivs-channel-tagged
- ivs-playback-key-pair-etiquetado
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado

- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted

- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro

- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled

- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3 -rules-check express-dir-bucket-lifecycle
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado

- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-plan de respaldo
- vpc-default-security-group-cerrado
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región de Europa (Londres)

Europa (Londres)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id

- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check

- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged

- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-creación de perfiles
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo

- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target

- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged

- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl

- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar

- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar

- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description

- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged

- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc

- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged

- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

Región Europa (Milán)

Europa (Milán)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check

- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled

- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-descansar
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled

- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required

- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached

- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit

- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado

- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar

- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- macie-auto-sensitive-data-descubrimiento-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización

- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia

- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support

- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled

- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check

- s3- meets-restore-time-target
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms

- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled

- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región Europa (París)

Europa (París)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar

- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged

- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-comprobación de tipos
- apprunner-service-max-unhealthy-umbral
- apprunner-service-no-public-acceso
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged

- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto

- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado

- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip

- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description

- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el balanceo
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe

- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled

- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar

- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled

- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan

- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado

- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled

- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión

- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description

- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región Europa (España)

Europa (España)

- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check

- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged

- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado

- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2-stopped-instance

- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-verificación de cifrado
- elastic-beanstalk-managed-updates-habilitado
- elbv2-multiple-az
- elb-cross-zone-load-habilitado para el equilibrio
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo

- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-habilitado
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-comprobar
- mariadb-publish-logs-to-cloudwatch-logs
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-habilitado para el registro
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged

- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar

- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled

- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región Europa (Estocolmo)

Europa (Estocolmo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged

- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged

- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-descansar
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check

- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización

- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado

- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default

- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to

- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración

- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para la autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el equilibrio
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo

- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado

- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar

- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-habilitado
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- lightsail-bucket-allow-public-anula- desactivado
- lightsail-bucket-tagged

- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-detección-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación

- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch

- rds-automatic-minor-version-habilitado para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged

- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3 -rules-check express-dir-bucket-lifecycle
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan

- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso

- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región Europa (Zúrich)

Europa (Zúrich)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra

- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-group-elb-healthcheck-obligatorio

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm

- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado

- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached

- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-verificación de cifrado
- elbv2-multiple-az
- elb-cross-zone-load-habilitado para el equilibrio
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar

- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-external-access-analyzer-habilitado
- iam-password-policy
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- mariadb-publish-logs-to-cloudwatch-logs
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado

- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitado para la actualización
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado

- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre

- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-encrypted-en tránsito
- redshift-serverless-workgroup-no-acceso público
- redshift-serverless-workgroup-routes-dentro del vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3

- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región Israel (Tel Aviv)

Israel (Tel Aviv)

- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description

- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-graphql-api-xray-habilitado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-registro
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-sCifrado en 3 registros
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged

- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar

- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- prefix-list-tagged
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -etiquetado transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-file-system-tagged
- efs-in-backup-plan
- efs-mount-target-public-accesible
- eip-attached
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elbv2-multiple-az
- elb-cross-zone-load-habilitado para el equilibrio

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-lustre-copy-tags-copias de seguridad
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-windows-deployment-type-comprobar
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado

- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- kinesis-firehose-delivery-stream-encriptado
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- macie-auto-sensitive-data-descubrimiento-comprobación
- mariadb-publish-logs-to-registros de cloudwatch
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled

- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes fragmentados
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-habilitado para el registro
- rds-automatic-minor-version-habilitada para la actualización
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar

- rds-in-backup-plan
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-no-acceso público
- redshift-unrestricted-port-access

- required-tags
- restricted-incoming-traffic
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- lifecycle-policy-check
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-no-public-acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- subnet-auto-assign-public-ip deshabilitado
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- webacl-not-empty
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región de México (centro)

México (centro)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-verificación de redireccionamiento
- apigatewayv2-stage-description
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-execution-logging-habilitado
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- cloudformation-stack-drift-detection-comprobar
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- cw-loggroup-retention-period-comprobar
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-comprobar
- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-acceso
- eks-secrets-encrypted

- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-comprobar
- emr-kerberos-enabled
- emr-master-no-public-ip
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-para su eliminación
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- multi-region-cloud-trail-habilitado
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-in-backup-plan
- rds-logging-enabled
- required-tags
- restricted-incoming-traffic
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-blacklisted-actions-prohibited
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3

- s3- bucket-ssl-requests-only
- s3- default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip deshabilitado
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Región Medio Oriente (Baréin)

Middle East (Bahrain)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged

- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged

- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento
- appconfig-hosted-configuration-version-descripción
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-en reposo
- appsync-cache-ct-encryption-en tránsito
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description

- athena-workgroup-description
- athena-workgroup-encrypted-at-descansar
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check

- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar

- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize

- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan

- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración

- ecs-task-definition-memory-límite estricto
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el equilibrio
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-openzfs-copy-tags-habilitado
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado

- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación

- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- macie-auto-sensitive-data-descubrimiento-comprobación
- macie-status-check
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch

- opensearch-node-to-node-comprobación de cifrado
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitado para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito

- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-a Cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc

- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged

- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-default-security-group-cerrado
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty

- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región Medio Oriente (EAU)

Medio Oriente (EAU)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled

- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-envvar-awscred-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado

- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm

- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged

- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-managed-updates-habilitado
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el equilibrio
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad

- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-habilitado
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-habilitado

- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar
- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitado para la actualización
- rds-cluster-default-admin-comprobar

- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-no-acceso público
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- ruta 53- resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3

- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío

Región de América del Sur (São Paulo)

América del Sur (São Paulo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deshabilitado
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-habilitado para el encabezado
- alb-http-to-https-verificación de redireccionamiento
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-habilitado para eliminar
- amplify-app-description
- amplify-app-no-environment-variables

- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-habilitado
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-habilitado
- apigateway-stage-description
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gwv2- -habilitado para métricas stage-default-route-detailed
- api-gw-associated-with-guerra
- api-gw-cache-enabled-y encriptado
- api-gw-endpoint-type-comprobar
- api-gw-execution-logging-habilitado
- api-gw-rest-api-etiquetado
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-no está vacío
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-a-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-almacenamiento

- appconfig-hosted-configuration-version-descripción
- appflow-flow-tagged
- appflow-flow-trigger-type-comprobar
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-reenvío
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-en reposo
- appsync-cache-ct-encryption-en tránsito
- appsync-cache-encryption-at-descanso
- appsync-graphql-api-xray-habilitado
- appsync-logging-enabled
- aps-rule-groups-namespace-etiquetado
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-descanso
- athena-workgroup-enforce-workgroup-configuración
- athena-workgroup-engine-version-actualización automática
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-en reposo
- aurora-last-backup-recovery-punto creado
- aurora-meets-restore-time-objetivo
- aurora-mysql-cluster-audit-registro
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-plan de respaldo
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-obligatorio
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-límite
- autoscaling-launch-config-public-ip-deshabilitado
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged

- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-habilitado
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-comprobar
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-comprobar
- codebuild-project-envvar-awscred-comprobar

- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-project-source-repo-comprobar la URL
- codebuild-report-group-encrypted-en reposo
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-habilitado
- codedeploy-deployment-group-auto-habilitado para la reversión
- codedeploy-deployment-group-outdated-instancias-actualización
- código deploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-desactivado
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-inicios de sesión
- cognito-identity-pool-unauth-control de acceso
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-habilitado para la seguridad
- cognito-user-pool-deletion-protección habilitada
- cognito-user-pool-mfa-habilitado
- cognito-user-pool-password-verificación de políticas
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-adjunto
- cw-loggroup-retention-period-comprobar
- datasync-location-object-storage-usando-https
- datasync-task-data-verification-habilitado
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-verificación de actualizaciones
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- dms-replication-task-sourcedb-registro
- dms-replication-task-tagged
- dms-replication-task-targetdb-registro
- docdb-cluster-audit-logging-habilitado
- docdb-cluster-backup-retention-comprobar
- docdb-cluster-deletion-protection-habilitado
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-tránsito
- docdb-cluster-snapshot-public-prohibido
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-meets-restore-time-objetivo
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-punto creado
- ebs-meets-restore-time-objetivo
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- capacity-reservation-tagged
- ec2- -habilitado client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -todos client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- 2-check launch-template-imdsv
- ec2- -desactivado launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -check managedinstance-association-compliance-status

- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- -análisis-etiquetado network-insights-access-scope
- ec2- network-insights-access-scope -etiquetado
- ec2- network-insights-analysis-tagged
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -gapped-vault resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periódico security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deshabilitado transit-gateway-auto-vpc
- ec2- transit-gateway-multicast-domain -etiquetado
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ec2- vpn-connection-tagged
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado

- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-no-environment-secrets
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuración
- ecs-task-definition-memory-límite estricto
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-usuario
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-directorio raíz
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-meets-restore-time-objetivo
- efs-mount-target-public-accesible

- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versión
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-auto-minor-version-verificación de actualizaciones
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticache-repl-grp-auto-habilitado para la conmutación por error
- elasticache-repl-grp-encrypted-en reposo
- elasticache-repl-grp-encrypted-en tránsito
- elasticache-repl-grp-redis-habilitado para autenticación
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-comprobación de cifrado
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-habilitado
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-habilitado para el equilibrio
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-comprobar
- elb-tagged
- elb-tls-https-listeners-solo
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-descansar
- emr-security-configuration-encryption-tránsito
- encrypted-volumes
- event-data-store-cmk-habilitado para el cifrado
- fis-experiment-template-log-configuración- existe
- fis-experiment-template-tagged
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-lustre-copy-tags-copias de seguridad
- fsx-meets-restore-time-objetivo
- fsx-ontap-deployment-type-comprobar

- fsx-openzfs-copy-tags-habilitado
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-audit-log-configurado
- fsx-windows-deployment-type-comprobar
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-habilitado
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-ml-transform-tagged
- glue-spark-job-supported-versión
- guardduty-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-habilitado
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-external-access-analyzer-habilitado
- iam-group-has-users-comprobar
- iam-inline-policy-blocked-kms-acciones
- iam-no-inline-policy-comprobar
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-comprobar
- iam-root-access-key-comprobar
- iam-user-group-membership-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- internet-gateway-authorized-vpc-solo
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-habilitado
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-retención de datos
- kms-cmk-not-scheduled-para su eliminación
- kms-key-policy-no-acceso público
- kms-key-tagged
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibido
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-comprobar
- macie-auto-sensitive-data-descubrimiento-comprobación
- macie-status-check
- mariadb-publish-logs-to-registros de cloudwatch
- mfa-enabled-for-iam-acceso a la consola
- mq-active-broker-ldap-autenticación
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-habilitada para la actualización
- mq-auto-minor-version-habilitada para la actualización
- mq-broker-general-logging-habilitado
- mq-cloudwatch-audit-logging-habilitado
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deshabilitado
- msk-cluster-tagged
- msk-connect-connector-logging-habilitado
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-comprobar

- neptune-cluster-cloudwatch-log-habilitado para la exportación
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-habilitado
- neptune-cluster-encrypted
- neptune-cluster-iam-database-autenticación
- neptune-cluster-multi-az-habilitado
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibido
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-paquetes de fragmentos
- netfw-policy-default-action-paquetes completos
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-cross-zone-load-habilitado para el equilibrio
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerancia
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-comprobación de cifrado

- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-habilitado para el registro
- rds-aurora-postgresql-logs-a cloudwatch
- rds-automatic-minor-version-habilitado para la actualización
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-comprobar
- rds-cluster-deletion-protection-habilitado
- rds-cluster-encrypted-at-descansar
- rds-cluster-iam-authentication-habilitado
- rds-cluster-multi-az-habilitado
- rds-db-security-group-no permitido
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-comprobar
- rds-instance-deletion-protection-habilitado
- rds-instance-iam-authentication-habilitado
- rds-instance-public-access-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-meets-restore-time-objetivo
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-en tránsito
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check

- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-proxy-tls-encryption
- rds-resources-protected-by-plan de respaldo
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-vigilancia en la nube
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-parameter-group-etiquetado
- redshift-cluster-public-access-comprobar
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-comprobar
- redshift-enhanced-vpc-routing-habilitado
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-serverless-publish-logs--to-cloudwatch
- redshift-serverless-workgroup-no-acceso público
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-habilitado
- root-account-mfa-enabled
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged
- s3- -solo access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques account-level-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-default-lock-enabled
- s3- bucket-level-public-access -prohibido
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled

- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -bóveda con huecos
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-etiquetado
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-instance-root-control de acceso
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-comprobar
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organización

- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-habilitada para notificaciones
- sns-topic-no-public-acceso
- sqs-queue-dlq-check
- sqs-queue-no-public-acceso
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-habilitado para el registro
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-comprobar
- vpc-peering-dns-resolution-comprobar
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-vacío
- waf-regional-rule-not-vacío
- waf-regional-webacl-not-vacío
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado
- workspaces-workspace-tagged

AWS GovCloud Región (EE. UU.-Este)

AWS GovCloud (Este de EE. UU.)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-verificación de redireccionamiento
- api-gw-execution-logging-habilitado
- api-gw-ssl-enabled

- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-punto creado
- aurora-mysql-cluster-audit-registro
- aurora-resources-protected-by-plan de respaldo
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- clb-desync-mode-check
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado

- codebuild-project-environment-privileged-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-report-group-encrypted-en reposo
- cw-loggroup-retention-period-comprobar
- datasync-task-logging-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- docdb-cluster-encrypted-in-tránsito
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado
- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- -habilitado client-vpn-connection-log
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-imdsv2-check
- ec2- -ami instance-launched-with-allowed

- ec2- instance-managed-by-ssm
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -plan resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecs-capacity-provider-termination-comprobar
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted

- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-mount-target-public-accesible
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-habilitado
- elbv2- listener-encryption-in-transit
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-comprobar
- elb-predefined-security-policy-ssl-comprobar
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-habilitado para el cifrado
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-deployment-type-comprobar

- glue-job-logging-enabled
- glue-spark-job-supported-versión
- guardduty-eks-protection-audit-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-inline-policy-blocked-kms-acciones
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-comprobar
- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- lambda-function-public-access-prohibido
- lambda-function-xray-enabled
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-acceso a la consola

- mq-cloudwatch-audit-log-habilitado
- msk-cluster-public-access-deshabilitado
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-cloudwatch
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-mysql-instance-encrypted-en tránsito
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-resources-protected-by-plan de respaldo
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-a Cloudwatch
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check

- redshift-cluster-multi-az-habilitado
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- solo s3- access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- habilitado para bucket-cross-region-replication s3
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check

- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- sqs-queue-dlq-check
- sqs-queue-policy-full-control de acceso
- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

AWS GovCloud Región (EE. UU.-Oeste)

AWS GovCloud (Estados Unidos-Oeste)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-verificación de redireccionamiento
- api-gw-execution-logging-habilitado
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-punto creado
- aurora-mysql-cluster-audit-registro
- aurora-resources-protected-by-plan de respaldo
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-eliminación-deshabilitada
- backup-recovery-point-minimum-control de retención
- clb-desync-mode-check
- cloudformation-stack-drift-detection-comprobar
- cloudformation-stack-service-role-comprobar
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- rastro de nubes - s3- bucket-access-logging

- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-habilitado para registros
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-habilitado para la validación
- cmk-backing-key-rotation-habilitado
- codebuild-project-environment-privileged-comprobar
- codebuild-project-logging-enabled
- codebuild-project-s3 registros cifrados
- codebuild-report-group-encrypted-en reposo
- cognito-identity-pool-unauth-control de acceso
- connect-instance-logging-enabled
- cw-loggroup-retention-period-comprobar
- datasync-task-logging-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-habilitado
- dms-neptune-iam-authorization-habilitado
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-habilitado
- dms-replication-not-public
- docdb-cluster-encrypted-in-tránsito
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punto creado

- dynamodb-resources-protected-by-plan de respaldo
- dynamodb-table-deletion-protection-habilitado
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punto creado
- ebs-resources-protected-by-plan de respaldo
- ebs-snapshot-block-public-acceso
- ebs-snapshot-public-restorable-comprobar
- ec2- -habilitado client-vpn-connection-log
- ec2- ebs-encryption-by-default
- ec2- -habilitado enis-source-destination-check
- ec2-imdsv2-check
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- -creado last-backup-recovery-point
- ec2- encriptado launch-templates-ebs-volume
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -check managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -plan resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-habilitado
- ecr-private-lifecycle-policy-configurado
- ecr-private-tag-immutability-habilitado
- ecr-repository-cmk-encryption-habilitado
- ecs-capacity-provider-termination-comprobar

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versión
- ecs-task-definition-efs-habilitado para el cifrado
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-identidad de usuario
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-punto creado
- efs-mount-target-public-accesible
- efs-resources-protected-by-plan de respaldo
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-acceso
- eks-secrets-encrypted
- elasticache-automatic-backup-check-habilitado
- elasticache-redis-cluster-automatic-verificación de respaldo
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-habilitado
- elbv2- listener-encryption-in-transit
- elbv2- -check predefined-security-policy-ssl
- elb-acm-certificate-required

- elb-custom-security-policy-ssl-comprobar
- elb-predefined-security-policy-ssl-comprobar
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-habilitado para el cifrado
- fms-shield-resource-policy-comprobar
- fms-webacl-resource-policy-comprobar
- fms-webacl-rulegroup-association-comprobar
- fsx-last-backup-recovery-punto creado
- fsx-ontap-deployment-type-comprobar
- fsx-openzfs-deployment-type-comprobar
- fsx-resources-protected-by-plan de respaldo
- fsx-windows-deployment-type-comprobar
- glue-job-logging-enabled
- glue-ml-transform-encrypted-en reposo
- glue-spark-job-supported-versión
- guardduty-eks-protection-audit-habilitado
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-acciones
- iam-inline-policy-blocked-kms-acciones
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-comprobar
- iam-server-certificate-expiration-comprobar

- iam-user-mfa-enabled
- iam-user-unused-credentials-comprobar
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-habilitado
- instances-in-vpc
- kinesis-firehose-delivery-stream-encriptado
- kinesis-stream-backup-retention-comprobar
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-para su eliminación
- lambda-function-public-access-prohibido
- lambda-function-xray-enabled
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-acceso a la consola
- mq-cloudwatch-audit-log-habilitado
- msk-cluster-public-access-deshabilitado
- msk-unrestricted-access-check
- multi-region-cloud-trail-habilitado
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-asociado
- netfw-stateless-rule-group-no está vacío
- netfw-subnet-change-protection-habilitado
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerancia
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-cloudwatch
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-comprobar
- rds-instance-subnet-igw-comprobar
- rds-in-backup-plan
- rds-last-backup-recovery-punto creado
- rds-logging-enabled
- rds-mariadb-instance-encrypted-en tránsito
- rds-mysql-instance-encrypted-en tránsito
- rds-postgresql-logs-to- vigilancia en la nube
- rds-postgres-instance-encrypted-en tránsito
- rds-resources-protected-by-plan de respaldo
- rds-sqlserver-encrypted-in-tránsito
- rds-sql-server-logs-a Cloudwatch
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-habilitado
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-require-tls-ssl
- redshift-serverless-default-admin-comprobar
- redshift-serverless-default-db-comprobar el nombre
- redshift-serverless-namespace-cmk-cifrado
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- solo s3- access-point-in-vpc
- s3- -bloques access-point-public-access
- s3- -bloques-periódicos account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited

- habilitado para bucket-cross-region-replication s3
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisivo
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- habilitado para bucket-server-side-encryption s3
- s3- bucket-ssl-requests-only
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- last-backup-recovery-point -creado
- s3- lifecycle-policy-check
- s3- resources-protected-by-backup -plan
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-configurado por clave
- sagemaker-endpoint-config-prod-recuento de instancias
- sagemaker-notebook-instance-kms-configurado por clave
- sagemaker-notebook-instance-platform-versión
- sagemaker-notebook-no-direct-acceso a internet
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organización
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sqs-queue-dlq-check
- sqs-queue-policy-full-control de acceso

- ssm-automation-block-public-compartir
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-punto creado
- storagegateway-resources-protected-by-plan de respaldo
- subnet-auto-assign-public-ip deshabilitado
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-punto creado
- virtualmachine-resources-protected-by-plan de respaldo
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-comprobar
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- workspaces-root-volume-encryption-habilitado
- workspaces-user-volume-encryption-habilitado

Creación de reglas AWS Config administradas con AWS CloudFormation plantillas

> **Important**
>
> Primero debe crear e iniciar el grabador de AWS Config configuración para poder crear reglas AWS Config administradas con AWS CloudFormation. Para obtener más información, consulte Administración del registrador de configuración.

Si necesita reglas AWS Config administradas compatibles, puede usar las CloudFormation plantillas para crear la regla para su cuenta o actualizar una CloudFormation pila existente. Una pila de es una colección de recursos relacionados que usted aprovisiona y actualiza como una única unidad. Al

iniciar una pila con una plantilla, la regla administrada por AWS Config se crea automáticamente. Las plantillas crean solo la regla y no crean AWS recursos adicionales.

> **Note**
>
> Cuando se actualizan las reglas AWS Config administradas, las plantillas se actualizan para adaptarse a los cambios más recientes. Para guardar una versión específica de una plantilla para una regla, descargue la plantilla y cárguela en su bucket de S3.

Para obtener más información sobre cómo trabajar con AWS CloudFormation plantillas, consulte Introducción a ellas AWS CloudFormation en la Guía del AWS CloudFormation usuario.

Para lanzar una CloudFormation pila de una regla AWS Config gestionada

1. Ve a la CloudFormationconsola y crea una pila nueva.
2. En Specify template (Especificar plantilla):
   - Si ha descargado la plantilla Upload a template file (Cargue un archivo de plantilla) y, a continuación, Choose file (Seleccionar archivo) para cargar la plantilla.
   - También puede elegir Amazon S3 URL y especificar la URL de ejemplo `http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template`.

   > **Note**
   >
   > El identificador de la regla debe escribirse en ALL_CAPS_WITH_UNDERSCORES. Por ejemplo, CLOUDWATCH_LOG_GROUP_ENCRYPTED en lugar de. cloudwatch-log-group-encrypted
   > En algunas reglas, el identificador de la regla es diferente del nombre de la regla. Asegúrese de usar el identificador de la regla. Por ejemplo, el identificador de la regla de restricted-ssh es INCOMING_SSH_DISABLED.

3. Elija Siguiente.
4. En Especificar los detalles de la pila, escriba un nombre de pila e introduzca los valores de los parámetros de la regla. AWS Config Por ejemplo, si utiliza la plantilla de reglas administradas `DESIRED_INSTANCE_TYPE`, puede especificar el tipo de instancia, como "m4.large".

5. Elija Siguiente.
6. En Options, puede crear etiquetas o configurar otras opciones avanzadas. Estas opciones no son obligatorias.
7. Elija Siguiente.
8. En Review (Revisar), compruebe que la plantilla, los parámetros y otras opciones son correctos.
9. Seleccione Crear. La pila se crea en unos minutos. Puede ver la regla creada en la consola de AWS Config.

Puede usar las plantillas para crear una pila única para las reglas AWS Config administradas o actualizar una pila existente en su cuenta. Si elimina una pila, las reglas administradas que se hayan creado a partir de esa pila también se eliminarán. Para obtener más información, consulte Trabajo con pilas en la Guía del usuario de AWS CloudFormation .

AWS Config Reglas personalizadas

AWS Config Las reglas personalizadas son reglas que se crean desde cero. Hay dos formas de crear reglas AWS Config personalizadas: con funciones de Lambda (Guía para AWS Lambda desarrolladores) y con Guard (Guard GitHub Repository), un policy-as-code lenguaje.

AWS Config las reglas personalizadas creadas con Lambda se denominan reglas AWS Config Lambda AWS Config personalizadas y las reglas personalizadas creadas con Guard se denominan AWS Config reglas de políticas personalizadas.

Antes de utilizar reglas personalizadas, consulte Consideraciones.

AWS Config Reglas de políticas personalizadas

Las reglas escritas con Guard se pueden crear desde la AWS Config consola o mediante la AWS Config regla APIs. AWS Config Las reglas de políticas personalizadas le permiten crear reglas AWS Config personalizadas sin necesidad de usar Java o Python para desarrollar funciones Lambda para administrar sus reglas personalizadas. AWS Config Las reglas de políticas personalizadas se inician mediante cambios en la configuración. Para obtener más información sobre Guard, consulte el GitHubrepositorio de Guard.

AWS Config Reglas Lambda personalizadas

Las reglas Lambda personalizadas ofrecen la opción de usar Java o Python para crear una función Lambda para una regla personalizada. AWS Config Una función Lambda es un código personalizado

en el que se carga y se invoca mediante eventos publicados en ella por una fuente de eventos. AWS Lambda Si la función Lambda está asociada a una AWS Config regla, la AWS Config invoca cuando se inicia la regla. A continuación, la función Lambda evalúa la información de configuración que envía y devuelve los AWS Config resultados de la evaluación. Para obtener más información sobre las funciones de Lambda, consulte Function and Event Sources en la Guía para desarrolladores de AWS Lambda .

Diferencias de formato para las reglas personalizadas AWS Config

En la siguiente tabla se muestran las diferencias de formato en los campos del tipo de ConfigurationItemdatos y de las reglas AWS Config personalizadas.

ConfigurationItem	AWS Config Regla personalizada
`version`	`configurationItemVersion`
`accountId`	`awsAccountId`
`arn`	`ARN`
`configurationItemMD5Hash`	`configurationStateMd5Hash`

Temas

- Creación de reglas de políticas AWS Config personalizadas
- Creación de AWS Config reglas Lambda personalizadas
- Administración de recursos eliminados para AWS Config reglas Lambda personalizadas

Creación de reglas de políticas AWS Config personalizadas

Puede crear reglas de política AWS Config personalizadas desde la Consola de administración de AWS AWS CLI, o la AWS Config API.

Añadir reglas de política AWS Config personalizadas

Using the console

1. Inicia sesión en la AWS Config consola de https://console.aws.amazon.com/config/tu casa Consola de administración de AWS y ábrela.

2. En el Consola de administración de AWS menú, compruebe que el selector de regiones esté configurado en una AWS región que admita AWS Config reglas. Para ver una lista de las regiones admitidas, consulte AWS Config Regions and Endpoints en la Referencia general de Amazon Web Services.
3. En el panel de navegación izquierdo, seleccione Rules (Reglas).
4. En la página Rules (Reglas), seleccione Add rule (Añadir regla).
5. En la página Especificar tipo de regla, elija Crear una regla personalizada con Guard.
6. En la página Configurar regla, cree la regla siguiendo estos pasos:
   a. En Nombre, escriba un nombre único para la regla.
   b. En Descripción, escriba una descripción para la regla.
   c. Para la versión de tiempo de ejecución de Guard, elija el sistema de tiempo de ejecución para su regla de política AWS Config personalizada.
   d. Para Contenido de la regla, puede indicar la política personalizada de Guard correspondiente a su regla.
   e. Para el modo de evaluación, elija en qué momento del proceso de creación y administración de recursos AWS Config desea evaluar sus recursos. Según la regla, AWS Config puede evaluar las configuraciones de sus recursos antes de aprovisionar un recurso, después de aprovisionar un recurso o ambas cosas.
      i. Elija Active la evaluación proactiva para ejecutar evaluaciones de los valores de configuración de sus recursos antes de que se implementen.

         Una vez que hayas activado la evaluación proactiva, puedes usar la StartResourceEvaluationAPI y la GetResourceEvaluationSummaryAPI para comprobar si los recursos que especificas en estos comandos se marcarán como NO CONFORMES según las reglas proactivas de tu cuenta en tu región.

         Para obtener más información sobre el uso de estos comandos, consulta Cómo evaluar tus recursos con reglas. AWS Config Para obtener una lista de reglas administradas que admiten una evaluación proactiva, consulte la Lista de reglas AWS Config administradas por modo de evaluación.
      ii. Seleccione Active la evaluación de detectives para evaluar los ajustes de la configuración de los recursos existentes.

Para una evaluación detectivesca, las reglas de política AWS Config personalizadas se inician mediante cambios en la configuración. Esta opción estará preseleccionada.

- Recursos: cuando se crea, cambia o elimina un recurso específico que coincide con un tipo de recurso específico o con un tipo más el identificador.
- Etiquetas: cuando se crea, cambia o elimina un recurso con la etiqueta especificada.
- Todos los cambios: cuando AWS Config se crea, modifica o elimina un recurso registrado por.

AWS Config ejecuta la evaluación cuando detecta un cambio en un recurso que coincide con el alcance de la regla. Puede utilizar el ámbito para restringir qué recursos inician evaluaciones. De lo contrario, las evaluaciones se inician cuando se produce un cambio en un recurso aprovisionado posteriormente.

f. Si su regla incluye Parámetros, puede personalizar los valores de las claves proporcionadas. Un parámetro es un atributo que deben cumplir los recursos para que se considere que cumplen la regla.

7. En la página Revisar y crear, revise todas las selecciones antes de añadir la regla a la Cuenta de AWS.
8. Cuando termine de revisar las reglas, seleccione Agregar regla.

Using the AWS CLI

Utilice el comando `put-config-rule`.

El campo `Owner` debe ser `CUSTOM_POLICY`. Los siguientes campos adicionales son obligatorios para las reglas de política AWS Config personalizada:

- `Runtime`: El sistema de ejecución de sus reglas de política AWS Config personalizada.
- `PolicyText`: definición de la política que contiene la lógica de las reglas de políticas personalizadas de AWS Config .
- `EnableDebugLogDelivery`: La expresión booleana para habilitar el registro de depuración para la regla de política AWS Config personalizada. El valor predeterminado es `false`.

Using the API Reference

Utilice la acción PutConfigRule.

El campo `Owner` debe ser `CUSTOM_POLICY`. Los siguientes campos adicionales son obligatorios para las reglas de política AWS Config personalizada:

- `Runtime`: El sistema de ejecución de sus reglas de política AWS Config personalizada.
- `PolicyText`: definición de la política que contiene la lógica de las reglas de políticas personalizadas de AWS Config .
- `EnableDebugLogDelivery`: La expresión booleana para habilitar el registro de depuración para la regla de política AWS Config personalizada. El valor predeterminado es `false`.

Escribir el contenido de las reglas de las políticas personalizadas AWS Config

Con las reglas de políticas AWS Config personalizadas, puede usar el lenguaje específico de dominio (DSL) de AWS CloudFormation Guard para evaluar las configuraciones de los recursos. En este tema se proporcionan patrones y prácticas recomendadas para escribir reglas de políticas personalizadas.

Para obtener más información sobre cómo escribir reglas con Guard, consulte Cómo escribir reglas de Guard en la Guía del usuario de AWS CloudFormation Guard y los modos de funcionamiento de AWS CloudFormation Guard 2.0 en el repositorio de Guard. GitHub

Estructura básica de reglas

Utilice el siguiente formato básico para crear reglas:

```
# Basic rule format
rule <rule_name> when
    resourceType == "<AWS::Service::Resource>" {
    # Evaluation clauses
}

# Example with filtering
let resources_of_type = Resources.*[ Type == 'AWS::Service::Resource' ]
rule check_resources when %resources_of_type !empty {
    %resources_of_type.configuration.property == expected_value
}
```

Componentes principales

configuración

Incluye el contenido de la configuración de recursos.

supplementaryConfiguration

Contiene contenido adicional para la configuración de recursos. AWS Config devuelve este campo para determinados tipos de recursos a fin de complementar la información devuelta para el campo de configuración.

resourceType

AWS tipo de recurso que se está evaluando.

resourceId

ID del recurso (por ejemplo, `sg-xxxxxx`).

accountId

El Cuenta de AWS identificador de 12 dígitos asociado al recurso.

Patrones comunes

Status checks

```
let allowed_status = ['ACTIVE', 'RUNNING']
rule check_resource_status when
    resourceType == "AWS::Service::Resource" {
    configuration.status IN %allowed_status
}
```

Required properties

```
rule check_required_properties when
    resourceType == "AWS::Service::Resource" {
    configuration.propertyName exists
    configuration.propertyName is_string  # or is_list, is_struct
}
```

Query blocks

```
configuration.Properties {
```

```
    property1 exists
    property2 is_string
    property3 IN [allowed_value1, allowed_value2]
}
```

Conditional evaluation

```
when configuration.feature_enabled == true {
    configuration.feature_settings exists
    configuration.feature_settings is_struct
}
```

Custom messages

```
rule check_compliance when
    resourceType == "AWS::Service::Resource" {
    configuration.property == expected_value <<Custom error message explaining the
 requirement>>
}}
```

Características avanzadas

Range checks

```
rule check_numeric_limits {
    # Inclusive range (lower_limit <= value <= upper_limit)
    configuration.value IN r[minimum_value, maximum_value]

    # Exclusive range (lower_limit < value < upper_limit)
    configuration.value IN r(exclusive_min, exclusive_max)

    # Left inclusive, right exclusive (lower_limit <= value < upper_limit)
    configuration.value IN r[minimum_value, exclusive_max)

    # Left exclusive, right inclusive (lower_limit < value <= upper_limit)
    configuration.value IN r(exclusive_min, maximum_value]
}
```

Combining conditions

```
# AND conditions (implicit through new lines)
```

```
condition_1
condition_2

# OR conditions (explicit)
condition_3 OR
condition_4
```

Chaining rules

```
rule check_prerequisites {
    configuration.required_setting exists
}

rule check_details when check_prerequisites {
    configuration.required_setting == expected_value
}
```

Prácticas recomendadas

- Utilice variables con instrucciones `let` para mejorar la legibilidad.
- Agrupe comprobaciones relacionadas mediante bloques de reglas con nombre.
- Incluya comentarios descriptivos.
- Utilice operadores adecuados (`exists`, `is_string`, `is_list`).
- Utilice patrones de expresiones regulares sin distinción entre mayúsculas y minúsculas.

Ejemplo: dynamodb-pitr-enabled

El siguiente ejemplo muestra la definición de política para una versión de regla de política AWS Config personalizada de la regla AWS Config dynamodb-pitr-enabled administrada. Esta regla comprueba si las tablas Point-in-Time de DynamoDB tienen habilitada la recuperación.

```
# Check if DynamoDB tables have Point-in-Time Recovery enabled
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}
```

```
rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
    let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription.pointIn
    %pitr == "ENABLED" <<DynamoDB tables must have Point-in-Time Recovery enabled>>
}
```

Creación de AWS Config reglas Lambda personalizadas

Puede desarrollar reglas personalizadas y añadirlas AWS Config con AWS Lambda funciones.

Cada regla personalizada se asocia a una función Lambda, que contiene la lógica que evalúa si los AWS recursos cumplen con la regla. Se asocia esta función a la regla y la regla invoca la función en respuesta a los cambios de configuración, o bien de forma periódica. A continuación, la función evalúa si los recursos cumplen con la regla y envía los resultados de la evaluación a. AWS Config

AWS Kit de desarrollo de reglas (RDK)

El kit de desarrollo de AWS reglas (RDK) está diseñado para respaldar un flujo de trabajo basado en el «cumplimiento según el código», que es intuitivo y productivo. Elimina gran parte del trabajo pesado e indiferenciado asociado a la implementación de AWS Config reglas respaldadas por funciones Lambda personalizadas y proporciona un proceso iterativo simplificado. develop-deploy-monitor

Para obtener step-by-step instrucciones, consulte la documentación del kit de desarrollo de AWS reglas (RDK).

Ejemplos de AWS Lambda funciones para AWS Config reglas (Node.js)

AWS Lambda ejecuta funciones en respuesta a eventos publicados por los AWS servicios. La función de una regla Lambda AWS Config personalizada recibe un evento publicado por y AWS Config, a continuación, utiliza los datos que recibe del evento y que recupera de la AWS Config API para evaluar el cumplimiento de la regla. Las operaciones que hay en una función de una regla de configuración son diferentes en función de si realiza una evaluación que se activa por los cambios en la configuración o se activa de forma periódica.

Para obtener información sobre los patrones comunes dentro de AWS Lambda las funciones, consulte el Modelo de programación en la Guía AWS Lambda para desarrolladores.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config invocará una función como la del ejemplo siguiente cuando detecte un cambio en la configuración de un recurso que esté dentro del ámbito de una regla personalizada.

Si usa la AWS Config consola para crear una regla asociada a una función como en este ejemplo, elija Cambios de configuración como tipo de activación. Si usa la AWS Config API o AWS CLI para crear la regla, defina el `MessageType` atributo en `ConfigurationItemChangeNotification` y`OversizedConfigurationItemChangeNotification`. Estos ajustes permiten que la regla se active cada vez que se AWS Config genere un elemento de configuración o un elemento de configuración sobredimensionado como resultado de un cambio de recurso.

En este ejemplo, se evalúan los recursos y se comprueba si las instancias coinciden con el tipo de recurso: `AWS::EC2::Instance`. La regla se activa cuando AWS Config genera un elemento de configuración o una notificación de un elemento de configuración sobredimensionado.

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory
 API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
```

```
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem)
 => {
```

```
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}

// In this example, the resource is compliant if it is an instance and its type
 matches the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration,
 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
```

```
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is
not compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
```

```
};
```

Operaciones de funciones

La función realiza las siguientes operaciones en tiempo de ejecución:

1. La función se ejecuta cuando AWS Lambda pasa el `event` objeto a la `handler` función. En este ejemplo, la función acepta el `callback` parámetro opcional, que utiliza para devolver información a la persona que llama. AWS Lambda también pasa un `context` objeto, que contiene información y métodos que la función puede utilizar mientras se ejecuta. Tenga en cuenta que en las versiones más recientes de Lambda, el contexto ya no se usa.
2. La función comprueba si el `messageType` del evento es un elemento de configuración o un elemento de configuración sobredimensionado y, a continuación, devuelve el elemento de configuración.
3. El controlador llama a la función `isApplicable` para determinar si el recurso se ha eliminado.

   > **Note**
   >
   > Las reglas que informen sobre los recursos eliminados deben devolver el resultado de la evaluación de `NOT_APPLICABLE` para evitar evaluaciones innecesarias de las reglas.

4. El controlador llama a la `evaluateChangeNotificationCompliance` función y pasa los `ruleParameters` objetos `configurationItem` y AWS Config publicados en el evento.

   La función evalúa primero si el recurso es una instancia EC2. Si el recurso no es una instancia EC2, la función devuelve un valor de conformidad de `NOT_APPLICABLE`.

   Luego, la función evalúa si el atributo `instanceType` del elemento de configuración es igual al valor del parámetro `desiredInstanceType`. Si los valores son iguales, la función devuelve `COMPLIANT`. Si los valores no son iguales, la función devuelve `NON_COMPLIANT`.
5. El controlador se prepara para enviar los resultados de la evaluación AWS Config inicializando el objeto. `putEvaluationsRequest` Este objeto incluye el parámetro `Evaluations`, que identifica el resultado de conformidad, el tipo de recurso y el ID del recurso que se ha evaluado. El `putEvaluationsRequest` objeto también incluye el token de resultados del evento, que identifica la regla y el evento. AWS Config
6. El controlador envía los resultados de la evaluación pasando el objeto al `putEvaluations` método del `config` cliente. AWS Config

Example Function for Periodic Evaluations

AWS Config invocará una función como la del siguiente ejemplo para las evaluaciones periódicas. Las evaluaciones periódicas se producen con la frecuencia que especifique al definir la regla en AWS Config.

Si usa la AWS Config consola para crear una regla asociada a una función como en este ejemplo, elija Periódico como tipo de activación. Si usa la AWS Config API o AWS CLI para crear la regla, defina el `MessageType` atributo en`ScheduledNotification`.

En este ejemplo, se comprueba si el número total de un recurso especificado supera un máximo especificado.

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON
 objects passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
 numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount,
 count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not
 compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
```

```
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
```

```
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource
 type.", null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count,
 callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
```

```
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
}
```

Operaciones de funciones

La función realiza las siguientes operaciones en tiempo de ejecución:

1. La función se ejecuta cuando AWS Lambda pasa el `event` objeto a la `handler` función. En este ejemplo, la función acepta el `callback` parámetro opcional, que utiliza para devolver información a la persona que llama. AWS Lambda también pasa un `context` objeto, que contiene información y métodos que la función puede utilizar mientras se ejecuta. Tenga en cuenta que en las versiones más recientes de Lambda, el contexto ya no se usa.
2. Para contar los recursos del tipo especificado, el controlador llama a la función `countResourceTypes` y pasa el parámetro `applicableResourceType` que ha recibido del evento. La función `countResourceTypes` llama al método `listDiscoveredResources` del cliente `config`, que devuelve una lista de identificadores para los recursos aplicables. La función utiliza la longitud de esta lista para determinar el número de recursos aplicables y devuelve este número al controlador.
3. El controlador se prepara para enviar los resultados de la evaluación AWS Config inicializando el `putEvaluationsRequest` objeto. Este objeto incluye el `Evaluations` parámetro, que identifica el resultado de conformidad y el Cuenta de AWS que se publicó en el evento. Puede utilizar el parámetro `Evaluations` para aplicar el resultado a cualquier tipo de recurso admitido por AWS Config. El `putEvaluationsRequest` objeto también incluye el token de resultado del evento, que identifica la regla y el evento AWS Config.
4. En el objeto `putEvaluationsRequest`, el controlador llama a la función `evaluateCompliance`. Esta función comprueba si el número de recursos aplicables supera el máximo asignado al parámetro `maxCount`, proporcionado anteriormente por el evento. Si el número de recursos supera el máximo, la función devuelve `NON_COMPLIANT`. Si el número de recursos no supera el máximo, la función devuelve `COMPLIANT`.
5. El controlador envía los resultados de la evaluación pasando el objeto al `putEvaluations` método del `config` cliente. AWS Config

Ejemplos de AWS Lambda funciones para AWS Config reglas (Python)

AWS Lambda ejecuta funciones en respuesta a eventos publicados por los AWS servicios. La función de una regla Lambda AWS Config personalizada recibe un evento publicado por y AWS Config, a continuación, utiliza los datos que recibe del evento y que recupera de la AWS Config API para evaluar el cumplimiento de la regla. Las operaciones que hay en una función de una regla de configuración son diferentes en función de si realiza una evaluación que se activa por los cambios en la configuración o se activa de forma periódica.

Para obtener información sobre los patrones comunes dentro de AWS Lambda las funciones, consulte el Modelo de programación en la Guía AWS Lambda para desarrolladores.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config invocará una función como la del ejemplo siguiente cuando detecte un cambio en la configuración de un recurso que esté dentro del ámbito de una regla personalizada.

Si usa la AWS Config consola para crear una regla asociada a una función como en este ejemplo, elija Cambios de configuración como tipo de activación. Si usa la AWS Config API o AWS CLI para crear la regla, defina el `MessageType` atributo en `ConfigurationItemChangeNotification` y`OversizedConfigurationItemChangeNotification`. Estos ajustes permiten que la regla se active cada vez que se AWS Config genere un elemento de configuración o un elemento de configuración sobredimensionado como resultado de un cambio de recurso.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
```

```
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] =
 json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
```

```
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'],
 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
```

```
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
```

```
                'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
                'ComplianceType': compliance_value,
                'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
            },
        ],
        ResultToken=event['resultToken'])
```

Operaciones de funciones

La función realiza las siguientes operaciones en tiempo de ejecución:

1. La función se ejecuta cuando AWS Lambda pasa el `event` objeto a la `handler` función. En este ejemplo, la función acepta el `callback` parámetro opcional, que utiliza para devolver información a la persona que llama. AWS Lambda también pasa un `context` objeto, que contiene información y métodos que la función puede utilizar mientras se ejecuta. Tenga en cuenta que en las versiones más recientes de Lambda, el contexto ya no se usa.
2. La función comprueba si el `messageType` del evento es un elemento de configuración o un elemento de configuración sobredimensionado y, a continuación, devuelve el elemento de configuración.
3. El controlador llama a la función `isApplicable` para determinar si el recurso se ha eliminado.

   > **Note**
   >
   > Las reglas que informen sobre los recursos eliminados deben devolver el resultado de la evaluación de `NOT_APPLICABLE` para evitar evaluaciones innecesarias de las reglas.

4. El controlador llama a la `evaluateChangeNotificationCompliance` función y pasa los `ruleParameters` objetos `configurationItem` y AWS Config publicados en el evento.

   La función evalúa primero si el recurso es una instancia EC2. Si el recurso no es una instancia EC2, la función devuelve un valor de conformidad de `NOT_APPLICABLE`.

   Luego, la función evalúa si el atributo `instanceType` del elemento de configuración es igual al valor del parámetro `desiredInstanceType`. Si los valores son iguales, la función devuelve `COMPLIANT`. Si los valores no son iguales, la función devuelve `NON_COMPLIANT`.

5. El controlador se prepara para enviar los resultados de la evaluación AWS Config inicializando el objeto. `putEvaluationsRequest` Este objeto incluye el parámetro `Evaluations`, que identifica el resultado de conformidad, el tipo de recurso y el ID del recurso que se ha evaluado. El `putEvaluationsRequest` objeto también incluye el token de resultados del evento, que identifica la regla y el evento. AWS Config
6. El controlador envía los resultados de la evaluación pasando el objeto al `putEvaluations` método del `config` cliente. AWS Config

Example Function for Periodic Evaluations

AWS Config invocará una función como la del siguiente ejemplo para las evaluaciones periódicas. Las evaluaciones periódicas se producen con la frecuencia que especifique al definir la regla en AWS Config.

Si usa la AWS Config consola para crear una regla asociada a una función como en este ejemplo, elija Periódico como tipo de activación. Si usa la AWS Config API o AWS CLI para crear la regla, defina el `MessageType` atributo en`ScheduledNotification`.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
```

```
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value
 to the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters
```

```
# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled
 rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report
 on the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])
        valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
```

```
        result_resource_count =
count_resource_types(valid_rule_parameters['applicableResourceType'], '',
resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
ResultToken=event['resultToken'])
```

Operaciones de funciones

La función realiza las siguientes operaciones en tiempo de ejecución:

1. La función se ejecuta cuando AWS Lambda pasa el `event` objeto a la `handler` función. En este ejemplo, la función acepta el `callback` parámetro opcional, que utiliza para devolver información a la persona que llama. AWS Lambda también pasa un `context` objeto, que contiene información y métodos que la función puede utilizar mientras se ejecuta. Tenga en cuenta que en las versiones más recientes de Lambda, el contexto ya no se usa.
2. Para contar los recursos del tipo especificado, el controlador llama a la función `countResourceTypes` y pasa el parámetro `applicableResourceType` que ha recibido del evento. La función `countResourceTypes` llama al método `listDiscoveredResources` del cliente `config`, que devuelve una lista de identificadores para los recursos aplicables. La función utiliza la longitud de esta lista para determinar el número de recursos aplicables y devuelve este número al controlador.
3. El controlador se prepara para enviar los resultados de la evaluación AWS Config inicializando el `putEvaluationsRequest` objeto. Este objeto incluye el `Evaluations` parámetro, que identifica el resultado de conformidad y el Cuenta de AWS que se publicó en el evento. Puede utilizar el parámetro `Evaluations` para aplicar el resultado a cualquier tipo de recurso admitido por AWS Config. El `putEvaluationsRequest` objeto también incluye el token de resultado del evento, que identifica la regla y el evento AWS Config.
4. En el objeto `putEvaluationsRequest`, el controlador llama a la función `evaluateCompliance`. Esta función comprueba si el número de recursos aplicables supera el máximo asignado al parámetro `maxCount`, proporcionado anteriormente por el evento. Si el número de recursos supera el máximo, la función devuelve `NON_COMPLIANT`. Si el número de recursos no supera el máximo, la función devuelve `COMPLIANT`.

5. El controlador envía los resultados de la evaluación pasando el objeto al `putEvaluations` método del `config` cliente. AWS Config

Ejemplos de eventos para reglas AWS Config

Cuando se produce el desencadenador de una regla, AWS Config invoca la AWS Lambda función de la regla publicando un evento. A continuación, AWS Lambda ejecuta la función pasando el evento al controlador de la función.

Example Event for Evaluations Triggered by Configuration Changes

AWS Config publica un evento cuando detecta un cambio en la configuración de un recurso que está dentro del ámbito de una regla. El siguiente ejemplo de evento muestra que la regla se ha activado por un cambio de configuración en una instancia EC2.

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Example Event for Evaluations Triggered by Oversized Configuration Changes

Algunos cambios de recursos generan elementos de configuración sobredimensionados. El siguiente ejemplo de evento muestra que la regla se ha activado por un cambio de configuración sobredimensionado en una instancia EC2.

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Example Event for Evaluations Triggered by Periodic Frequency

AWS Config publica un evento cuando evalúa sus recursos con la frecuencia que especifique (por ejemplo, cada 24 horas). El siguiente evento de ejemplo muestra que la regla se ha activado por una frecuencia periódica.

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime
\":\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",
\"recordVersion\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
```

```
}
```

Atributos del evento

El objeto JSON de un AWS Config evento contiene los siguientes atributos:

`invokingEvent`

El evento que dispara la evaluación de una regla. Si el evento se publica en respuesta a un cambio de configuración de recurso, el valor de este atributo es una cadena que contiene un `configurationItem` JSON o un `configurationItemSummary` (para elementos de configuración sobredimensionados). El elemento de configuración representa el estado del recurso en el momento en que AWS Config se detectó el cambio. Para ver un ejemplo de un elemento de configuración, consulte el resultado generado por el `get-resource-config-history` AWS CLI comando enVisualización del historial de configuración.

Si el evento se publica para una evaluación periódica, el valor es una cadena que contiene un objeto JSON. El objeto incluye información sobre la evaluación que se ha activado.

Para cada tipo de evento, una función debe analizar la cadena con un analizador JSON para poder evaluar su contenido, tal y como se muestra en el siguiente ejemplo Node.js:

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

Pares clave/valor que la función procesa como parte de su lógica de evaluación. Los parámetros se definen cuando se utiliza la AWS Config consola para crear una regla Lambda personalizada. También puede definir los parámetros con el `InputParameters` atributo de la solicitud de `PutConfigRule` AWS Config API o el `put-config-rule` AWS CLI comando.

El código JSON de los parámetros está almacenado dentro de una cadena, por lo que una función debe analizar la cadena con un analizador JSON para poder evaluar su contenido, tal y como se muestra en el siguiente ejemplo Node.js:

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

Un token al que la función debe pasar AWS Config con la `PutEvaluations` llamada.

`eventLeftScope`

Un valor booleano que indica si el AWS recurso que se va a evaluar se ha eliminado del ámbito de la regla. Si el valor es `true`, la función indica que la evaluación se puede pasar por alto aprobando `NOT_APPLICABLE` como el valor para el atributo `ComplianceType` en la llamada `PutEvaluations`.

`executionRoleArn`

El ARN de la función de IAM a la que está asignada. AWS Config

`configRuleArn`

El ARN que se AWS Config asignó a la regla.

`configRuleName`

El nombre que asignó a la regla que provocó AWS Config la publicación del evento y la invocación de la función.

`configRuleId`

El ID que se AWS Config asignó a la regla.

`accountId`

El ID del propietario Cuenta de AWS de la regla.

`version`

Un número de versión asignado por AWS. La versión aumentará si AWS agrega atributos a los AWS Config eventos. Si una función requiere un atributo que solo está en eventos que cumplan o superen una versión específica, entonces esa función puede comprobar el valor de este atributo.

La versión actual para los AWS Config eventos es la 1.0.

Administración de recursos eliminados para AWS Config reglas Lambda personalizadas

Las reglas que informen sobre los recursos eliminados deben devolver el resultado de la evaluación de `NOT_APPLICABLE` para evitar evaluaciones innecesarias de las reglas.

Al eliminar un recurso, AWS Config crea un `configurationItem` ancho `ResourceDeleted` para el`configurationItemStatus`. Puede utilizar estos metadatos para comprobar si una

regla informa sobre un recurso eliminado. Para obtener más información sobre los elementos de configuración, consulte Conceptos | Elementos de configuración.

Incluye los siguientes fragmentos de código para comprobar si hay recursos eliminados y establecer el resultado de la evaluación de una regla lambda AWS Config personalizada en `NOT_APPLICABLE` caso de que informe sobre un recurso eliminado:

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config Las reglas administradas y las reglas de política AWS Config personalizadas controlan este comportamiento de forma predeterminada.

Si crea una regla lambd AWS Config personalizada con Python mediante el kit de AWS Config desarrollo (RDK) y la biblioteca del kit de AWS Config desarrollo (RDKlib), la clase Evaluator importada comprobará este comportamiento. Para obtener información sobre cómo escribir reglas con el RDK RDKlib, consulte Escribir reglas con el RDK y. RDKlib

Roles vinculados a servicios de AWS Config

Una regla vinculada al servicio de AWS Config es un tipo único de regla administrada de AWS Config compatible con otros servicios de AWS para crear reglas de AWS Config en su cuenta. Las reglas vinculadas a servicios están predefinidas para incluir todos los permisos necesarios para llamar a otros servicios de AWS en su nombre. Estas reglas son similares a las normas que un servicio de AWS recomienda en su Cuenta de AWS para una verificación de conformidad.

Estas reglas de AWS Config vinculadas al servicio son propiedad de los equipos del servicio de AWS. El equipo del servicio de AWS crea estas reglas en su Cuenta de AWS. Tiene acceso de solo lectura a estas reglas. No se puede editar ni eliminar estas reglas si se ha suscrito al servicio de AWS al que estas reglas están vinculadas.

Reglas vinculadas a servicios y la AWS Command Line Interface

Con la AWS CLI, las API PutConfigRule, DeleteConfigRule y DeleteEvaluationResults devuelven el acceso denegado con el siguiente mensaje de error:

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

Reglas vinculadas a servicios y la consola de AWS Config

En la consola de AWS Config, las reglas vinculadas al servicio de AWS Config se pueden ver en la página Reglas. Los botones Editar y Eliminar los resultados aparecen en gris en la consola para impedir la edición de la regla. Puede ver los detalles de la regla eligiendo la regla.

Reglas vinculadas a servicios, acciones de corrección y paquetes de conformidad

Para añadir acciones de corrección a las reglas vinculadas a un servicio de un paquete de conformidad, debe añadir la acción de corrección a la propia plantilla del paquete de conformidad y, a continuación, actualizar el paquete de conformidad con la plantilla actualizada. Para obtener

más información sobre la actualización de los paquetes de conformidad, consulte Deploying a Conformance Pack (Console), Deploying a Conformance Pack (AWS CLI) y Managing Organizational Conformance Packs.

Edición y eliminación de roles vinculados a servicios

Para editar o eliminar una regla vinculada a un servicio, póngase en contacto con el servicio de AWS que ha creado la regla. Por ejemplo, en el caso de las reglas vinculadas a servicios creadas por AWS Security Hub CSPM, puede eliminar una regla vinculada a un servicio siguiendo estos pasos en la Guía del usuario de AWS Security Hub CSPM: Disabling a security standard.

Administración de AWS Config reglas en todas las cuentas de su organización

> **Important**
>
> Las reglas de la organización solo se pueden crear con la API o la CLI. Esta operación no es compatible con la AWS Config consola.

AWS Config permite gestionar las AWS Config reglas en todos los Cuentas de AWS ámbitos de una organización. Puede:

- Cree, actualice y elimine AWS Config reglas de forma centralizada en todas las cuentas de su organización.
- Implemente un conjunto común de AWS Config reglas en todas las cuentas y especifique las cuentas en AWS Config las que no se deben crear reglas.
- APIs Utilícelas desde la cuenta de administración AWS Organizations para reforzar la gobernanza, asegurándose de que las cuentas de los miembros de su organización no puedan modificar las AWS Config reglas subyacentes.

Consideraciones

Para implementaciones en diferentes regiones

La llamada a la API para implementar reglas y paquetes de conformidad en todas las cuentas es específica de cada AWS región. En el nivel de organización, debe cambiar el contexto de la llamada

a la API a una región diferente si quiere implementar reglas en otras regiones. Por ejemplo, para implementar una regla en Este de EE. UU. (Norte de Virginia), cambie la región a Este de EE. UU. (Norte de Virginia) y, a continuación, llame a `PutOrganizationConfigRule`.

Para cuentas dentro de una organización

Si una cuenta nueva se une a una organización, la regla o el paquete de conformidad se implementan en esa cuenta. Cuando una cuenta abandona una organización, se elimina la regla o el paquete de conformidad.

Si implementa una regla organizativa o un paquete de conformidad en una cuenta de administrador de la organización y, a continuación, establece un administrador delegado e implementa una regla organizativa o un paquete de conformidad en la cuenta de administrador delegado, no podrá ver la regla organizativa ni el paquete de conformidad en la cuenta de administrador de la organización desde la cuenta de administrador delegado ni ver la regla organizativa ni el paquete de conformidad en la cuenta de administrador delegado desde la cuenta de administrador de la organización. El DescribeOrganizationConfigRulesy solo DescribeOrganizationConformancePacks APIs puede ver e interactuar con los recursos relacionados con la organización que se implementaron desde la cuenta a la que se hace referencia. APIs

Mecanismo de reintento para las cuentas nuevas que se agreguen a una organización

Si no hay ningún registrador disponible, solo se volverán a intentar implementar las reglas organizativas y los paquetes de conformidad existentes durante 7 horas después de añadir una cuenta a su organización. Se espera que cree un registrador si no existe uno dentro de las 7 horas siguientes a la adición de una cuenta a su organización.

Cuentas de administración de la organización, administradores delegados y roles vinculados a servicios

Si utilizas una cuenta de administración de la organización y piensas usar un administrador delegado para el despliegue organizacional, ten en cuenta que eso AWS Config no creará automáticamente el rol vinculado al servicio (SLR). Debe crear el rol vinculado al servicio (SLR) manualmente y por separado, mediante IAM.

Si no tiene un SLR para la cuenta de administración, no podrá implementar recursos en esa cuenta desde una cuenta de administrador delegado. Podrás seguir implementando AWS Config reglas en las cuentas de los miembros desde las cuentas de administración y de administrador delegado. Para obtener más información, consulte Uso de roles vinculados a servicios en la Guía del usuario de AWS Identity and Access Management (IAM).

Implementación

Para obtener información sobre cómo realizar la integración AWS Config con AWS Organizations, consulte AWS Config y AWS Organizations en la Guía del AWS Organizations usuario. Asegúrese de que la AWS Config grabación esté activada antes de utilizar lo siguiente APIs para gestionar AWS Config las reglas Cuentas de AWS en toda la organización:

- PutOrganizationConfigRule, agrega o actualiza la regla de configuración de la organización para toda la organización y evalúa si sus AWS recursos cumplen con las configuraciones deseadas.
- DescribeOrganizationConfigRules, devuelve una lista de reglas de configuración de la organización.
- GetOrganizationConfigRuleDetailedStatus, devuelve el estado detallado de cada cuenta de miembro de una organización para una regla de configuración de la organización determinada.
- GetOrganizationCustomRulePolicy, devuelve la definición de política que contiene la lógica de la regla de política personalizada de configuración de la organización.
- DescribeOrganizationConfigRuleStatuses, proporciona el estado de despliegue de la regla de configuración de la organización para una organización.
- DeleteOrganizationConfigRule, elimina la regla de configuración de la organización especificada y todos los resultados de su evaluación de todas las cuentas de los miembros de esa organización.

Compatibilidad de la región

En las siguientes regiones se admite la implementación de AWS Config reglas en las cuentas de los miembros de una AWS organización.

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Este de EE. UU.	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
(Norte de Virginia)			
Oeste de EE. UU. (Norte de California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Tailandia)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
México (centro)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Añadir AWS Config reglas

Puede utilizar la AWS Config consola o la AWS SDKs para añadir reglas.

Temas

- Adición de reglas (consola)
- Añadir reglas (AWS SDKs)

Adición de reglas (consola)

La página Reglas muestra las reglas y los resultados de conformidad actuales en una tabla. El resultado de cada regla es Evaluando... hasta que AWS Config termine de evaluar sus recursos con respecto a la regla. Puede actualizar los resultados con el botón de actualizar. Cuando AWS Config finalicen las evaluaciones, podrá ver las reglas y los tipos de recursos que cumplen o no. Para obtener más información, consulte Visualización de la información de cumplimiento y los resultados de la evaluación de sus AWS recursos con AWS Config.

> **Note**
>
> Cuando agrega una nueva regla, AWS Config evalúa los recursos aplicables en su inventario de recursos, incluidos los recursos registrados anteriormente. Por ejemplo, si ha registrado `AWS::IoT::Policy` los recursos pero luego los ha excluido del registro, AWS Config conserva los elementos de configuración iniciales (CIs) de su inventario. Aunque ya AWS Config no los actualiza CIs cuando los tipos de recursos asociados no se registran, conserva su último estado registrado y los evalúa al añadir las reglas aplicables.

AWS Config no evalúa los recursos que no estén en el inventario de recursos. Por ejemplo, si agregas la amplify-branch-tagged regla pero no registras ni has registrado nunca `AWS::Amplify::Branch` los recursos, no AWS Config podrás evaluar si las AWS Amplify sucursales de tu cuenta cumplen con las normas o no.
Para obtener más información, consulte Grabación de AWS recursos con AWS Config.

Adición de reglas

Para añadir una regla

1. Inicia sesión en la AWS Config consola de https://console.aws.amazon.com/config/tu casa Consola de administración de AWS y ábrela.
2. En el Consola de administración de AWS menú, compruebe que el selector de región esté configurado en una región que admita AWS Config reglas. Para ver una lista de las regiones admitidas, consulte Regiones y puntos de enlace de AWS Config en la Referencia general de Amazon Web Services.
3. En el panel de navegación izquierdo, seleccione Rules (Reglas).
4. En la página Rules (Reglas), seleccione Add rule (Añadir regla).
5. En la página Especificar tipo de regla, especifique el tipo de regla siguiendo estos pasos:
   a. En el campo de búsqueda para filtrar escriba la lista de las reglas administradas por nombre de regla, descripción y etiqueta. Por ejemplo, escriba EC2 para que devuelva las reglas que evalúan tipos de recursos de EC2 o escriba periodic para que devuelva reglas que se activen periódicamente.
   b. También puede crear sus propia regla personalizada. Elija Crear regla personalizada con Lambda o Crear regla personalizada con Guard y siga el procedimiento descrito en Creación de reglas AWS Config Lambda personalizadas o Creación AWS Config de reglas de políticas personalizadas.
6. En la página Configurar regla, configure la regla siguiendo estos pasos:
   a. En Name (Nombre), escriba un nombre único para la regla.
   b. En Descripción, escriba una descripción para la regla.
   c. Para el modo de evaluación, elija en qué momento del proceso de creación y administración de recursos desea AWS Config evaluar sus recursos. Según la regla, AWS Config puede

evaluar las configuraciones de sus recursos antes de que se haya desplegado un recurso, después de que se haya desplegado un recurso, o ambas cosas.

i. Elija Active la evaluación proactiva para ejecutar evaluaciones de los valores de configuración de sus recursos antes de que se implementen.

   Una vez que hayas activado la evaluación proactiva, puedes usar la StartResourceEvaluationAPI y la GetResourceEvaluationSummaryAPI para comprobar si los recursos que especificas en estos comandos se marcarán como NO CONFORMES según las reglas proactivas de tu cuenta de tu región.

   Para obtener más información sobre el uso de estos comandos, consulta Cómo evaluar tus recursos con reglas. AWS Config Para obtener una lista de reglas administradas que admiten una evaluación proactiva, consulte la Lista de reglas AWS Config administradas por modo de evaluación.

ii. Seleccione Active la evaluación de detectives para evaluar los ajustes de la configuración de los recursos existentes.

   Para la evaluación de detectives, existen dos tipos de desencadenadores: Cuando cambia la configuración y Periódico.

   A. Si los tipos de desencadenadores de la regla incluyen cambios de configuración, especifique una de las siguientes opciones para el alcance de los cambios con la que se AWS Config invoca la función Lambda:

      - Recursos: cuando se crea, cambia o elimina un recurso específico que coincide con un tipo de recurso específico o con un tipo más el identificador.
      - Etiquetas: cuando se crea, cambia o elimina un recurso con la etiqueta especificada.
      - Todos los cambios: cuando AWS Config se crea, modifica o elimina un recurso registrado por.

      AWS Config ejecuta la evaluación cuando detecta un cambio en un recurso que coincide con el alcance de la regla. Puede utilizar el ámbito para definir los recursos que activan evaluaciones.

   B. Si los tipos de desencadenadores de la regla incluyen Periódico, especifique la frecuencia con la que se AWS Config invoca la función Lambda.

d. Si su regla incluye Parámetros, puede personalizar los valores de las claves proporcionadas. Un parámetro es un atributo que deben cumplir los recursos para que se considere que cumplen la regla.

7. En la página Revisar y crear, revise todas las selecciones antes de añadir la regla a la Cuenta de AWS. Si la regla no funciona según lo previsto, puede que vea una de las siguientes opciones para Conformidad:

   - No se informó de ningún resultado: AWS Config evaluó sus recursos según la regla. La regla no se aplicaba a los AWS recursos incluidos en su ámbito, se eliminaron los recursos especificados o se eliminaron los resultados de la evaluación. Para obtener los resultados de la evaluación, actualice la regla, cambie su ámbito o bien seleccione Re-evaluate (Volver a evaluar).

     Este mensaje también puede aparecer si la regla no informa de resultados de evaluación.
   - No hay recursos dentro del alcance: AWS Config no puede evaluar AWS los recursos registrados según esta regla porque ninguno de sus recursos está dentro del alcance de la regla. Para obtener los resultados de la evaluación, edite la regla y cambie su alcance, o añada recursos AWS Config para registrarlos mediante la página de configuración.
   - Evaluations failed (Error en las evaluaciones): para obtener información que le ayude a determinar el problema, elija el nombre de la regla para abrir la página de detalles y ver el mensaje de error.

Añadir reglas (AWS SDKs)

Adición de reglas

Los siguientes ejemplos de código muestran cómo utilizar `PutConfigRule`.

CLI

AWS CLI

Para añadir una regla de Config AWS gestionada

El siguiente comando proporciona código JSON para añadir una regla de Config AWS gestionada:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` es un archivo JSON que contiene la configuración de la regla:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Para el `ComplianceResourceTypes` atributo, este código JSON limita el alcance a los recursos de este `AWS::EC2::Instance` tipo, por lo que AWS Config evaluará solo las instancias de EC2 según la regla. Puesto que la regla es una regla administrada, el atributo `Owner` se establece en `AWS` y el atributo `SourceIdentifier` en el identificador de la regla, `REQUIRED_TAGS`. Para el atributo `InputParameters`, se especifican las claves de etiqueta que requiere la regla, `CostCenter` y `Owner`.

Si el comando se ejecuta correctamente, AWS Config no devuelve ningún resultado. Para verificar la configuración de la regla, ejecute el describe-config-rules comando y especifique el nombre de la regla.

Adición de una regla de configuración administrada por el cliente

En el siguiente comando se proporciona un código JSON para añadir una regla de configuración administrada por el cliente:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` es un archivo JSON que contiene la configuración de la regla:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Para el `ComplianceResourceTypes` atributo, este código JSON limita el alcance a los recursos de este `AWS::EC2::Instance` tipo, por lo que AWS Config evaluará solo las instancias de EC2 según la regla. Como esta regla es una regla administrada por el cliente, el `Owner` atributo se establece en y el `SourceIdentifier` atributo se establece en el ARN de la función Lambda AWS . `CUSTOM_LAMBDA` El objeto `SourceDetails` es obligatorio. Los parámetros que se especifican para el `InputParameters` atributo se pasan a la función AWS Lambda cuando AWS Config la invoca para evaluar los recursos en función de la regla.

Si el comando se ejecuta correctamente, AWS Config no devuelve ningún resultado. Para verificar la configuración de la regla, ejecute el describe-config-rules comando y especifique el nombre de la regla.

- Para obtener más información sobre la API, consulte PutConfigRulela Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
```

```
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Para obtener más información sobre la API, consulta PutConfigRulela AWS Referencia de API de SDK for Python (Boto3).

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    " Create a config rule for S3 bucket public read prohibition
    lo_cfs->putconfigrule(
      io_configrule = NEW /aws1/cl_cfsconfigrule(
        iv_configrulename = iv_rule_name
        iv_description = |S3 Public Read Prohibited Bucket Rule|
        io_scope = NEW /aws1/cl_cfsscope(
          it_complianceresourcetypes = VALUE /aws1/
cl_cfscplncresrctypes_w=>tt_complianceresourcetypes(
            ( NEW /aws1/cl_cfscplncresrctypes_w( |AWS::S3::Bucket| ) )
          )
        )
        io_source = NEW /aws1/cl_cfssource(
          iv_owner = |AWS|
          iv_sourceidentifier = |S3_BUCKET_PUBLIC_READ_PROHIBITED|
        )
```

```
        iv_inputparameters = '{}'
        iv_configrulestate = |ACTIVE|
      )
    ).
    MESSAGE 'Created AWS Config rule.' TYPE 'I'.
```

- Para obtener más información sobre la API, consulte PutConfigRulela referencia sobre la API ABAP del AWS SDK para SAP.

Actualización de AWS Config reglas

Puede utilizar la AWS Config consola o la AWS SDKs para actualizar las reglas.

Temas

- Actualización de reglas (consola)
- Actualización de reglas (AWS SDKs)

Actualización de reglas (consola)

La página Reglas muestra las reglas y los resultados de conformidad actuales en una tabla. El resultado de cada regla es Evaluar... hasta que AWS Config termine de evaluar sus recursos con respecto a la regla. Puede actualizar los resultados con el botón de actualizar. Cuando AWS Config finalicen las evaluaciones, podrá ver las reglas y los tipos de recursos que cumplen o no. Para obtener más información, consulte Visualización de la información de cumplimiento y los resultados de la evaluación de sus AWS recursos con AWS Config.

Actualización de reglas

Para actualizar una regla

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.
2. En el Consola de administración de AWS menú, compruebe que el selector de región esté configurado en una región que admita AWS Config reglas. Para ver una lista de las regiones admitidas, consulte Regiones y puntos de enlace de AWS Config en la Referencia general de Amazon Web Services.
3. En el panel de navegación izquierdo, seleccione Rules (Reglas).

4. Elija una regla y Editar la regla para la regla que desee actualizar.
5. Modifique la configuración de la página Editar la regla para cambiar la regla según sea necesario.
6. Seleccione Save.

Actualización de reglas (AWS SDKs)

Actualización de reglas

Si va a actualizar una regla que ha añadido anteriormente, puede especificar la regla por `ConfigRuleName`, `ConfigRuleId` o `ConfigRuleArn` en el tipo de datos `ConfigRule` que utiliza en esta solicitud. Se utiliza el mismo comando (`PutConfigRule`) que se utiliza al añadir una regla.

Los siguientes ejemplos de código muestran cómo utilizar `PutConfigRule`.

CLI

AWS CLI

Para añadir una regla de Config AWS gestionada

El siguiente comando proporciona código JSON para añadir una regla de Config AWS gestionada:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` es un archivo JSON que contiene la configuración de la regla:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
```

```
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Para el `ComplianceResourceTypes` atributo, este código JSON limita el alcance a los recursos de este `AWS::EC2::Instance` tipo, por lo que AWS Config evaluará solo las instancias de EC2 según la regla. Puesto que la regla es una regla administrada, el atributo `Owner` se establece en `AWS` y el atributo `SourceIdentifier` en el identificador de la regla, `REQUIRED_TAGS`. Para el atributo `InputParameters`, se especifican las claves de etiqueta que requiere la regla, `CostCenter` y `Owner`.

Si el comando se ejecuta correctamente, AWS Config no devuelve ningún resultado. Para verificar la configuración de la regla, ejecute el describe-config-rules comando y especifique el nombre de la regla.

Adición de una regla de configuración administrada por el cliente

En el siguiente comando se proporciona un código JSON para añadir una regla de configuración administrada por el cliente:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` es un archivo JSON que contiene la configuración de la regla:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
```

```
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Para el `ComplianceResourceTypes` atributo, este código JSON limita el alcance a los recursos de este `AWS::EC2::Instance` tipo, por lo que AWS Config evaluará solo las instancias de EC2 según la regla. Como esta regla es una regla administrada por el cliente, el `Owner` atributo se establece en y el `SourceIdentifier` atributo se establece en el ARN de la función Lambda AWS . `CUSTOM_LAMBDA` El objeto `SourceDetails` es obligatorio. Los parámetros que se especifican para el `InputParameters` atributo se pasan a la función AWS Lambda cuando AWS Config la invoca para evaluar los recursos en función de la regla.

Si el comando se ejecuta correctamente, AWS Config no devuelve ningún resultado. Para verificar la configuración de la regla, ejecute el describe-config-rules comando y especifique el nombre de la regla.

- Para obtener más información sobre la API, consulte PutConfigRulela Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
```

```
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Para obtener más información sobre la API, consulta PutConfigRulela AWS Referencia de API de SDK for Python (Boto3).

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    " Create a config rule for S3 bucket public read prohibition
    lo_cfs->putconfigrule(
      io_configrule = NEW /aws1/cl_cfsconfigrule(
        iv_configrulename = iv_rule_name
        iv_description = |S3 Public Read Prohibited Bucket Rule|
        io_scope = NEW /aws1/cl_cfsscope(
          it_complianceresourcetypes = VALUE /aws1/
cl_cfscplncresrctypes_w=>tt_complianceresourcetypes(
            ( NEW /aws1/cl_cfscplncresrctypes_w( |AWS::S3::Bucket| ) )
          )
        )
        io_source = NEW /aws1/cl_cfssource(
          iv_owner = |AWS|
          iv_sourceidentifier = |S3_BUCKET_PUBLIC_READ_PROHIBITED|
        )
        iv_inputparameters = '{}'
        iv_configrulestate = |ACTIVE|
      )
    ).
    MESSAGE 'Created AWS Config rule.' TYPE 'I'.
```

- Para obtener más información sobre la API, consulte PutConfigRulela referencia sobre la API ABAP del AWS SDK para SAP.

Eliminar AWS Config reglas

Puede usar la AWS Config consola o la AWS SDKs para eliminar sus reglas.

Temas

- Consideraciones
- Eliminación de reglas (consola)
- Eliminar reglas (AWS SDKs)

Consideraciones

Recomendación: considere excluir el tipo de recurso **`AWS::Config::ResourceCompliance`** del registro antes de eliminar reglas

Al eliminar las reglas, se crean elementos de configuración (CIs) `AWS::Config::ResourceCompliance` que pueden afectar a los costes del registrador de configuración. Si elimina reglas que evalúan un gran número de tipos de recursos, esto puede provocar un aumento en el número de CIs registros.

Para evitar los costos asociados, puede optar por deshabilitar el registro para el tipo de recurso `AWS::Config::ResourceCompliance` antes de eliminar reglas y volver a habilitarlo una vez eliminadas las reglas.

Sin embargo, dado que la eliminación de reglas es un proceso asincrónico, puede tardar una hora o más en completarse. Durante el tiempo en que el registro esté deshabilitado para `AWS::Config::ResourceCompliance`, las evaluaciones de reglas no se registrarán en el historial de recursos asociado.

Eliminación de reglas (consola)

La página Reglas muestra las reglas y los resultados de conformidad actuales en una tabla. El resultado de cada regla es Evaluar... hasta que AWS Config termine de evaluar sus recursos con respecto a la regla. Puede actualizar los resultados con el botón de actualizar. Cuando AWS Config finalicen las evaluaciones, podrá ver las reglas y los tipos de recursos que cumplen o no. Para obtener más información, consulte Visualización de la información de cumplimiento y los resultados de la evaluación de sus AWS recursos con AWS Config.

> **Note**
>
> AWS Config evalúa solo los tipos de recursos que está registrando. Por ejemplo, si agregas la regla habilitada para CloudTrail pero no registras el tipo de recurso de la CloudTrail ruta, no AWS Config podrás evaluar si las rutas de tu cuenta cumplen o no lo hacen. Para obtener más información, consulte Grabación de AWS recursos con AWS Config.

Eliminación de reglas

Para eliminar una regla

1. Inicia sesión en la consola de tu casa Consola de administración de AWS y ábrela AWS Config . https://console.aws.amazon.com/config/
2. En el Consola de administración de AWS menú, compruebe que el selector de región esté configurado en una región que admita AWS Config reglas. Para ver una lista de las regiones admitidas, consulte Regiones y puntos de enlace de AWS Config en la Referencia general de Amazon Web Services.
3. En el panel de navegación izquierdo, seleccione Rules (Reglas).
4. Elija la regla que desea eliminar de la tabla.
5. En el menú desplegable Acciones, elija Eliminar la regla.
6. Cuando se le pida, escriba Eliminar (distingue entre mayúsculas y minúsculas) y, a continuación, seleccione Eliminar.

Eliminar reglas (AWS SDKs)

Eliminación de reglas

Los siguientes ejemplos de código muestran cómo utilizar `DeleteConfigRule`.

CLI

AWS CLI

Para eliminar una regla de AWS Config

El siguiente comando elimina una regla de AWS Config denominada`MyConfigRule`:

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Para obtener más información sobre la API, consulte DeleteConfigRulela Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Para obtener más información sobre la API, consulta DeleteConfigRulela AWS Referencia de API de SDK for Python (Boto3).

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
lo_cfs->deleteconfigrule( iv_rule_name ).
MESSAGE 'Deleted AWS Config rule.' TYPE 'I'.
```

- Para obtener más información sobre la API, consulte DeleteConfigRulela referencia sobre la API ABAP del AWS SDK para SAP.

Visualización de los detalles y la información de cumplimiento de sus AWS Config reglas

> **Important**
>
> Para obtener informes precisos sobre el estado de cumplimiento, debe registrar el tipo de recurso de `AWS::Config::ResourceCompliance`. Para obtener más información, consulte AWS Recursos de grabación.

Puedes usar la AWS Config consola o la AWS SDKs para ver tus reglas.

Temas

- Visualización de las reglas (consola)
- Reglas de visualización (AWS SDKs)

Visualización de las reglas (consola)

La página Reglas muestra las reglas y los resultados de conformidad actuales en una tabla. El resultado de cada regla es Evaluar... hasta que AWS Config termine de evaluar sus recursos con

respecto a la regla. Puede actualizar los resultados con el botón de actualizar. Cuando AWS Config finalicen las evaluaciones, podrá ver las reglas y los tipos de recursos que cumplen o no. Para obtener más información, consulte Visualización de la información de cumplimiento y los resultados de la evaluación de sus AWS recursos con AWS Config.

> **Note**
>
> AWS Config evalúa solo los tipos de recursos que está registrando. Por ejemplo, si agregas la regla habilitada para CloudTrail pero no registras el tipo de recurso de la CloudTrail ruta, no AWS Config podrás evaluar si las rutas de tu cuenta cumplen o no lo hacen. Para obtener más información, consulte Grabación de AWS recursos con AWS Config.

Visualización de reglas

Para ver las reglas

1. Inicia sesión en la consola de tu casa Consola de administración de AWS y ábrela AWS Config . https://console.aws.amazon.com/config/
2. En el Consola de administración de AWS menú, compruebe que el selector de región esté configurado en una región que admita AWS Config reglas. Para ver una lista de las regiones admitidas, consulte Regiones y puntos de enlace de AWS Config en la Referencia general de Amazon Web Services.
3. En el panel de navegación izquierdo, seleccione Rules (Reglas).
4. La página de reglas muestra todas las reglas que tiene actualmente en su cuenta Cuenta de AWS. En ella se muestra el nombre, la acción correctiva asociada y el estado de conformidad de cada regla.
   - Elija Add rule (Añadir regla) para comenzar la creación de una regla.
   - Elija una regla para ver su configuración o elija una regla y Ver detalles.
   - Consulte el estado de conformidad de la regla cuando se evalúan los recursos.
   - Elija una regla y Editar la regla para cambiar los ajustes de configuración de la regla y establecer una acción correctiva para una regla no conforme.

Reglas de visualización (AWS SDKs)

Visualización de los detalles de las reglas

Los siguientes ejemplos de código muestran cómo utilizar `DescribeConfigRules`.

CLI

AWS CLI

Para obtener detalles de una regla de AWS Config

El siguiente comando devuelve los detalles de una regla de AWS Config denominada`InstanceTypesAreT2micro`:

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Salida:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
```

```
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeConfigRuleslla Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se enumeran las reglas de configuración de la cuenta, con las propiedades seleccionadas.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Salida:

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Para obtener más información sobre la API, consulte DescribeConfigRules Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se enumeran las reglas de configuración de la cuenta, con las propiedades seleccionadas.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Salida:

```
ConfigRuleName                                   ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                   ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                            config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                              config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required       config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Para obtener más información sobre la API, consulte DescribeConfigRuleslla referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class ConfigWrapper:
```

```
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Para obtener más información sobre la API, consulta DescribeConfigRuleslla AWS Referencia de API de SDK for Python (Boto3).

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    DATA(lo_result) = lo_cfs->describeconfigrules(
      it_configrulenames = VALUE /aws1/
cl_cfsconfigrulenames_w=>tt_configrulenames(
        ( NEW /aws1/cl_cfsconfigrulenames_w( iv_rule_name ) )
      )
    ).
    ot_cfg_rules = lo_result->get_configrules( ).
    MESSAGE 'Retrieved AWS Config rule data.' TYPE 'I'.
```

- Para obtener más información sobre la API, consulte DescribeConfigRuleslа referencia sobre la API ABAP del AWS SDK para SAP.

Visualización de información de conformidad para las reglas

Los siguientes ejemplos de código muestran cómo utilizar `DescribeComplianceByConfigRule`.

CLI

AWS CLI

Para obtener información sobre el cumplimiento de tus reglas de AWS Config

El siguiente comando devuelve la información de conformidad de cada regla de AWS Config que uno o más AWS recursos infrinjan:

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

En el resultado, el valor de cada atributo de `CappedCount` indica cuántos recursos no cumplen con la regla relacionada. Por ejemplo, el siguiente resultado indica que tres recursos no cumplen con la regla denominada `InstanceTypesAreT2micro`.

Salida:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeComplianceByConfigRulela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Este ejemplo recupera los detalles de conformidad de la regla ebs-optimized-instance, para los que no hay resultados de evaluación actuales, por lo que devuelve INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Salida:

```
ComplianceContributorCount ComplianceType
------------------------- --------------
                           INSUFFICIENT_DATA
```

Ejemplo 2: Este ejemplo devuelve el número de recursos no conformes para la regla ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Salida:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Para obtener más información sobre la API, consulte Cmdlet Reference (V4 DescribeComplianceByConfigRule).Herramientas de AWS para PowerShell

Herramientas para la versión 5 PowerShell

Ejemplo 1: Este ejemplo recupera los detalles de conformidad de la regla ebs-optimized-instance, para los que no hay resultados de evaluación actuales, por lo que devuelve INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Salida:

```
ComplianceContributorCount ComplianceType
------------------------- --------------
                           INSUFFICIENT_DATA
```

Ejemplo 2: Este ejemplo devuelve el número de recursos no conformes para la regla ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Salida:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Para obtener más información sobre la API, consulte Cmdlet Reference (V5 DescribeComplianceByConfigRule).Herramientas de AWS para PowerShell

Visualización del resumen de conformidad de las reglas

Los siguientes ejemplos de código muestran cómo utilizar `GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Para obtener el resumen de conformidad de tus reglas de AWS Config

El comando siguiente devuelve el número de reglas conformes y el de las reglas no conformes:

```
aws configservice get-compliance-summary-by-config-rule
```

En el resultado, el valor de cada atributo `CappedCount` indica el número de reglas conformes o no conformes.

Salida:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
```

```
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Para obtener más información sobre la API, consulta GetComplianceSummaryByConfigRulela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Este ejemplo devuelve el número de reglas de Config que no son conformes.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Salida:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByConfigRule Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Este ejemplo devuelve el número de reglas de Config que no son conformes.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Salida:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByConfigRulela referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Visualización de los resultados de la evaluación de las reglas

Los siguientes ejemplos de código muestran cómo utilizar `GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Para obtener los resultados de la evaluación de una regla de AWS Config

El siguiente comando devuelve los resultados de la evaluación de todos los recursos que no cumplen con una regla de AWS Config denominada`InstanceTypesAreT2micro`:

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Salida:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
```

```
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Para obtener más información sobre la API, consulta GetComplianceDetailsByConfigRulela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo se obtienen los resultados de la evaluación de la regla access-keys-rotated y se devuelve el resultado agrupado por tipo de conformidad

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Salida:

```
Count Name                      Group
----- ----                      -----
```

```
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Ejemplo 2: En este ejemplo se consultan los detalles de conformidad de la regla access-keys-rotated para los recursos de COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Salida:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Para obtener más información sobre la API, consulte GetComplianceDetailsByConfigRule Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo se obtienen los resultados de la evaluación de la regla access-keys-rotated y se devuelve el resultado agrupado por tipo de conformidad

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Salida:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Ejemplo 2: En este ejemplo se consultan los detalles de conformidad de la regla access-keys-rotated para los recursos de COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Salida:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Para obtener más información sobre la API, consulte GetComplianceDetailsByConfigRule Herramientas de AWS para PowerShellCmdlet Reference (V5).

Activar la evaluación proactiva de AWS Config las reglas

Puede utilizar la AWS Config consola o la AWS SDKs para activar las reglas de evaluación proactiva. Para obtener una lista de tipos de recursos y reglas administradas que admiten evaluación proactiva, consulte Componentes de una regla | Modos de evaluación.

Temas

- Activación de la evaluación proactiva (consola)
- Activar la evaluación proactiva ()AWS SDKs

Activación de la evaluación proactiva (consola)

La página Reglas muestra las reglas y los resultados de conformidad actuales en una tabla. El resultado de cada regla es Evaluar... hasta que AWS Config termine de evaluar sus recursos con respecto a la regla. Puede actualizar los resultados con el botón de actualizar.

Cuando AWS Config finalicen las evaluaciones, podrá ver las reglas y los tipos de recursos que cumplen o no. Para obtener más información, consulte Visualización de la información de cumplimiento y los resultados de la evaluación de sus AWS recursos con AWS Config.

> **Note**
>
> AWS Config evalúa solo los tipos de recursos que está registrando. Por ejemplo, si agregas la regla habilitada para CloudTrail pero no registras el tipo de recurso de la CloudTrail ruta, no AWS Config podrás evaluar si las rutas de tu cuenta cumplen o no lo hacen. Para obtener más información, consulte Grabación de AWS recursos con AWS Config.

Activación de la evaluación proactiva

Puede utilizar la evaluación proactiva para evaluar los recursos antes de que se implementen. Esto te permite evaluar si un conjunto de propiedades de un recurso, si se utiliza para definir un AWS recurso, cumple o no lo es, dado el conjunto de reglas proactivas que tienes en tu cuenta en tu región.

El Esquema de tipos de recurso indica las propiedades de un recurso. Puede encontrar el esquema del tipo de recurso en "extensiones AWS públicas" en el AWS CloudFormation registro o con el siguiente comando CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Para obtener más información, consulte Administración de extensiones mediante el CloudFormation registro y la referencia sobre los tipos de AWS recursos y propiedades en la Guía del AWS CloudFormation usuario.

> **Note**
>
> Las reglas proactivas no corrigen los recursos que están marcados como NON_COMPLIANT ni impiden su implementación.

Para activar una evaluación proactiva

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.
2. En el Consola de administración de AWS menú, compruebe que el selector de regiones esté configurado en una región que admita AWS Config reglas. Para ver una lista de las regiones de AWS admitidas, consulte AWS Config Regions and Endpoints en la Referencia general de Amazon Web Services.

3. En el panel de navegación izquierdo, seleccione Rules (Reglas). Para obtener una lista de reglas administradas que admiten una evaluación proactiva, consulte la Lista de reglas AWS Config administradas por modo de evaluación.
4. Elija una regla y, a continuación, elija Editar la regla para la regla que desee actualizar.
5. En Modo de evaluación, seleccione Active la evaluación proactiva para ejecutar evaluaciones de los valores de configuración de sus recursos antes de que se implementen.
6. Seleccione Save.

Una vez que haya activado la evaluación proactiva, puede utilizar la StartResourceEvaluationAPI y la GetResourceEvaluationSummaryAPI para comprobar si los recursos que especifique en estos comandos se marcarán como NO CONFORMES según las reglas proactivas de su cuenta de su región.

Por ejemplo, comience con la API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Debería recibir el `ResourceEvaluationId` en el resultado:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

A continuación, `ResourceEvaluationId` utilícela con la GetResourceEvaluationSummary API para comprobar el resultado de la evaluación:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Debería obtener un resultado similar al siguiente:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Para ver información adicional sobre el resultado de la evaluación, por ejemplo, qué regla marcó un recurso como NO CUMPLIDO, usa la API. GetComplianceDetailsByResource

Activar la evaluación proactiva ()AWS SDKs

Activación de la evaluación proactiva (AWS CLI)

Puede utilizar la evaluación proactiva para evaluar los recursos antes de que se implementen. Esto le permite evaluar si un conjunto de propiedades de un recurso, si se utiliza para definir un AWS recurso, cumpliría o no lo sería, dado el conjunto de reglas proactivas que tiene en su cuenta en su región.

El Esquema de tipos de recurso indica las propiedades de un recurso. Puede encontrar el esquema del tipo de recurso en "extensiones AWS públicas" en el AWS CloudFormation registro o con el siguiente comando CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Para obtener más información, consulte Administración de extensiones mediante el CloudFormation registro y la referencia sobre los tipos de AWS recursos y propiedades en la Guía del AWS CloudFormation usuario.

> **Note**
>
> Las reglas proactivas no corrigen los recursos que están marcados como NON_COMPLIANT ni impiden su implementación.

Para activar la evaluación proactiva

Utilice el comando `put-config-rule` y active `PROACTIVE` para `EvaluationModes`.

Una vez que haya activado la evaluación proactiva, puede usar el comando start-resource-evaluationCLI y el comando get-resource-evaluation-summaryCLI para comprobar si los recursos que especifique en estos comandos se marcarán como NO CONFORMES según las reglas proactivas de su cuenta en su región.

Por ejemplo, empiece con el comando start-resource-evaluation:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Debería recibir el `ResourceEvaluationId` en el resultado:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

A continuación, utilice el `ResourceEvaluationId` junto con el get-resource-evaluation-summary para comprobar el resultado de la evaluación:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Debería obtener un resultado similar al siguiente:

```
{
```

```
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Para ver información adicional sobre el resultado de la evaluación, por ejemplo, qué regla marcó un recurso como NON_COMPLIANT, utilice el comando CLI -resourceget-compliance-details-by.

> **Note**
>
> Para obtener una lista de reglas administradas que admiten una evaluación proactiva, consulte Lista de reglas AWS Config administradas por modo de evaluación.

Activación de la evaluación proactiva (API)

Puede utilizar la evaluación proactiva para evaluar los recursos antes de que se implementen. Esto le permite evaluar si un conjunto de propiedades de un recurso, si se utiliza para definir un AWS recurso, cumple o no cumple con las normas proactivas de las que dispone en su cuenta de su región.

El Esquema de tipos de recurso indica las propiedades de un recurso. Puede encontrar el esquema del tipo de recurso en "extensiones AWS públicas" en el AWS CloudFormation registro o con el siguiente comando CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Para obtener más información, consulte Administración de extensiones mediante el CloudFormation registro y la referencia sobre los tipos de AWS recursos y propiedades en la Guía del AWS CloudFormation usuario.

> **Note**
>
> Las reglas proactivas no corrigen los recursos que están marcados como NON_COMPLIANT ni impiden su implementación.

Para activar la evaluación proactiva para una regla

Utilice la PutConfigRuleacción y habilite `PROACTIVE` para`EvaluationModes`.

Una vez que hayas activado la evaluación proactiva, puedes usar la StartResourceEvaluationAPI y la GetResourceEvaluationSummaryAPI para comprobar si los recursos que especificas en estos comandos se marcarán como NO CONFORMES según las reglas proactivas de tu cuenta de tu región. Por ejemplo, comience con la API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Debería recibir el `ResourceEvaluationId` en el resultado:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

A continuación, `ResourceEvaluationId` utilícela con la GetResourceEvaluationSummary API para comprobar el resultado de la evaluación:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Debería obtener un resultado similar al siguiente:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
```

```
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Para ver información adicional sobre el resultado de la evaluación, por ejemplo, qué regla marcó un recurso como NO CUMPLIDO, usa la API. GetComplianceDetailsByResource

> **Note**
>
> Para obtener una lista de reglas administradas que admiten la evaluación proactiva, consulte la Lista de reglas AWS Config administradas por modo de evaluación.

Envío de evaluaciones de reglas a Security Hub (CSPM)

Después de añadir una AWS Config regla, también puede enviar las evaluaciones de la regla a. AWS Security Hub CSPM La integración entre Security Hub CSPM AWS Config y Security Hub le permite clasificar y corregir las evaluaciones de las reglas, junto con otros errores de configuración y problemas de seguridad.

Envíe las evaluaciones de las reglas a Security Hub (CSPM)

Para enviar evaluaciones de reglas a Security Hub CSPM, primero debe configurar AWS Security Hub CSPM y AWS Config, a continuación, agregar al menos una regla AWS Config administrada o personalizada. Después de esto, comienza AWS Config inmediatamente a enviar las evaluaciones de las reglas al Security Hub CSPM. Security Hub CSPM enriquece las evaluaciones de reglas y las transforma en hallazgos de Security Hub CSPM.

Para obtener más información sobre esta integración, consulte las integraciones de AWS servicios disponibles en la Guía del usuario. AWS Security Hub CSPM

Evaluación de sus recursos con AWS Config reglas

Cuando crea reglas personalizadas o utiliza reglas administradas, AWS Config evalúa sus recursos en función de esas reglas. Puede realizar evaluaciones bajo demanda de los recursos con respecto a sus reglas. Por ejemplo, esto resulta útil cuando se crea una regla personalizada y se desea comprobar si AWS Config se están evaluando correctamente los recursos o si hay algún problema con la lógica de evaluación de la AWS Lambda función.

Ejemplo

1. Puede crear una regla personalizada que evalúe si los usuarios de IAM tienen claves de acceso activas.
2. AWS Config evalúa los recursos en función de la regla personalizada.
3. Hay un usuario de IAM que no tiene una clave de acceso activa en su cuenta. La regla no marca correctamente este recurso como NON_COMPLIANT.
4. Puede corregir la regla y empezar de nuevo la evaluación.
5. Dado que ha corregido la regla, la regla evalúa correctamente los recursos y marca el recurso de usuario de IAM como NON_COMPLIANT.

Al agregar una regla a su cuenta, puede especificar en qué momento del proceso de creación y administración de recursos desea AWS Config evaluar sus recursos. El proceso de creación y administración de los recursos se denomina aprovisionamiento de recursos. Usted elige el modo de evaluación para especificar en qué momento de este proceso AWS Config desea evaluar sus recursos.

Según la regla, AWS Config puede evaluar las configuraciones de los recursos antes de que se haya desplegado un recurso, después de que se haya desplegado un recurso, o ambas cosas. Evaluar un recurso antes de implementarlo se denomina evaluación proactiva. Evaluar un recurso después de implementarlo se denomina evaluación de detectives.

Modo proactivo

Utilice una evaluación proactiva para evaluar los recursos antes de que se implementen. Esto le permite evaluar si un conjunto de propiedades de un recurso, si se utiliza para definir un AWS recurso, es conforme o no, dado el conjunto de reglas proactivas que tiene en su cuenta en su región.

El Esquema de tipos de recurso indica las propiedades de un recurso. Puede encontrar el esquema del tipo de recurso en "extensiones AWS públicas" en el AWS CloudFormation registro o con el siguiente comando CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Para obtener más información, consulte Administración de extensiones mediante el CloudFormation registro y la referencia sobre los tipos de AWS recursos y propiedades en la Guía del AWS CloudFormation usuario.

> **Note**
>
> Las reglas proactivas no corrigen los recursos que están marcados como NON_COMPLIANT ni impiden su implementación.

Evaluación de sus recursos

Para activar una evaluación proactiva

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.
2. En el Consola de administración de AWS menú, compruebe que el selector de regiones esté configurado en una región que admita AWS Config reglas. Para ver una lista de las regiones de AWS admitidas, consulte AWS Config Regions and Endpoints en la Referencia general de Amazon Web Services.
3. En el panel de navegación izquierdo, seleccione Rules (Reglas). Para obtener una lista de reglas administradas que admiten una evaluación proactiva, consulte la Lista de reglas AWS Config administradas por modo de evaluación.
4. Elija una regla y, a continuación, elija Editar la regla para la regla que desee actualizar.
5. En Modo de evaluación, seleccione Active la evaluación proactiva para ejecutar evaluaciones de los valores de configuración de sus recursos antes de que se implementen.
6. Seleccione Save.

> **Note**
>
> También puede activar la evaluación proactiva mediante el `put-config-rule`comando y habilitar `PROACTIVE` `EvaluationModes` o usar la PutConfigRuleacción y habilitar `PROACTIVE` for`EvaluationModes`.

Una vez que hayas activado la evaluación proactiva, puedes usar la StartResourceEvaluationAPI y la GetResourceEvaluationSummaryAPI para comprobar si los recursos que especifiques en estos comandos se marcarán como NO CONFORMES según las reglas proactivas de tu cuenta de tu región.

Por ejemplo, comience con la API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Debería recibir el `ResourceEvaluationId` en el resultado:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

A continuación, `ResourceEvaluationId` utilícela con la GetResourceEvaluationSummary API para comprobar el resultado de la evaluación:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Debería obtener un resultado similar al siguiente:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
```

```
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Para ver información adicional sobre el resultado de la evaluación, por ejemplo, qué regla marcó un recurso como NO CUMPLIDO, usa la API. GetComplianceDetailsByResource

Modo de detectives

Utilice la evaluación de detectives para evaluar los recursos que ya se han implementado. Esto le permite evaluar los ajustes de configuración de los recursos existentes.

Evaluación de sus recursos (consola)

1. Inicia sesión en la AWS Config consola de tu Consola de administración de AWS casa y ábrela. https://console.aws.amazon.com/config/
2. En el Consola de administración de AWS menú, comprueba que el selector de regiones esté configurado en una región que admita AWS Config reglas. Para ver una lista de las regiones admitidas, consulte Regiones y puntos de enlace de AWS Config en la Referencia general de Amazon Web Services.
3. En el panel de navegación, seleccione Reglas. La página Reglas muestra el nombre, la acción correctiva asociada y el estado de conformidad de cada regla.
4. Seleccione una regla de la tabla.
5. En la lista desplegable Acciones, seleccione Volver a evaluar.
6. AWS Config comienza a evaluar los recursos en función de tu regla.

> **Note**
>
> Puede volver a evaluar una regla una vez por minuto. Debe esperar AWS Config a que se complete la evaluación de la regla antes de iniciar otra evaluación. No puede ejecutar una evaluación si la regla se está actualizando al mismo tiempo o si la regla se está eliminando.

Evaluación de sus recursos (CLI)

- Utilice el comando start-config-rules-evaluation:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

AWS Config comienza a evaluar las configuraciones de recursos registradas en función de su regla. También puede especificar varias reglas en su solicitud:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

Evaluación de sus recursos (API)

Utilice la acción StartConfigRulesEvaluation.

Eliminar los resultados de la evaluación de AWS Config las reglas

Una vez AWS Config evaluada la regla, podrá ver los resultados de la evaluación en la página de reglas o en la página de detalles de la regla. Si los resultados de la evaluación son incorrectos o si desea realizar de nuevo la evaluación, puede eliminar los resultados de la evaluación actuales de la regla. Por ejemplo, si la regla estaba evaluando de forma incorrecta los recursos o recursos que se han eliminado recientemente de su cuenta, puede eliminar los resultados de la evaluación y, a continuación, ejecutar una nueva evaluación.

Deleting Evaluation Results (Console)

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.

2. En el Consola de administración de AWS menú, compruebe que el selector de regiones esté configurado en una AWS región que admita AWS Config reglas. Para ver una lista de las regiones admitidas, consulte AWS Config Regions and Endpoints en la Referencia general de Amazon Web Services.
3. En el panel de navegación, seleccione Reglas. La página Reglas muestra el nombre, la acción correctiva asociada y el estado de conformidad de cada regla.
4. Seleccione una regla de la tabla.
5. En el menú desplegable Acciones, elija Eliminar los resultados.
6. Cuando se le pida, escriba Eliminar (distingue entre mayúsculas y minúsculas) y, a continuación, elija Eliminar. Después de eliminar una evaluación, no podrá recuperarla.
7. Después de que los resultados de la evaluación se eliminen, puede iniciar manualmente una nueva evaluación.

Deleting Evaluation Results (CLI)

- Utilice el comando delete-evaluation-results.

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

  AWS Config elimina los resultados de la evaluación de la regla.

Deleting Evaluation Results (API)

Utilice la acción DeleteEvaluationResults.

Solución de problemas relacionados con las reglas AWS Config

Compruebe los siguientes problemas para solucionarlos si no puede eliminar una AWS Config regla o recibe un error similar al siguiente: «Se ha producido un error con AWS Config».

La entidad AWS Identity and Access Management (IAM) tiene permisos para la API DeleteConfigRule

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Usuarios o Roles.

3. Elija el usuario o el rol que utilizó para eliminar la AWS Config regla y amplíe las políticas de permisos.
4. En la pestaña Permisos, elija JSON.
5. En el panel de vista previa de JSON, confirme que la política de IAM permite permisos para la DeleteConfigRuleAPI.

El límite de permisos de la entidad de IAM permite la API DeleteConfigRule

Si la entidad de IAM tiene un límite de permisos, asegúrese de que permita los permisos para la DeleteConfigRule API.

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Usuarios o Roles.
3. Elija el usuario o el rol que utilizó para eliminar la AWS Config regla, amplíe el límite de permisos y, a continuación, elija JSON.
4. En el panel de vista previa de JSON, confirme que la política de IAM permite permisos para la DeleteConfigRuleAPI.

> **Warning**
>
> Los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo de seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

La política de control de servicios (SCP) permite la API DeleteConfigRule

1. Abra la AWS Organizations consola al https://console.aws.amazon.com/organizations/ usar la cuenta de administración de la organización.
2. En Nombre de cuenta, seleccione la Cuenta de AWS.
3. En Políticas, expanda Políticas de control de servicios (SCP) y anote las políticas SCP asociadas.
4. En la parte superior de la página, seleccione Políticas.
5. Seleccione la política y Ver detalles.
6. En el panel de vista previa de JSON, confirme que la política permita la DeleteConfigRuleAPI.

La regla no es una regla vinculada a un servicio

Cuando habilitas un estándar de seguridad, AWS Security Hub CSPM crea reglas vinculadas al servicio para ti. No puede eliminar estas reglas vinculadas a un servicio mediante AWS Config, y el botón de eliminación aparece atenuado. Para eliminar una regla vinculada a un servicio, consulte Desactivación de un estándar de seguridad en la Guía del usuario de CSPM de Security Hub.

No hay ninguna acción correctiva en curso

No puede eliminar AWS Config las reglas que tengan acciones correctivas en curso. Siga los pasos para eliminar la acción correctiva asociada a esa regla. A continuación, intente eliminar la regla de nuevo.

> **Important**
>
> Elimine únicamente las acciones correctivas que se encuentren en el estado Error o Correcto.

Paquetes de conformidad para AWS Config

Un paquete de conformidad es un conjunto de AWS Config reglas y medidas correctivas que se pueden implementar fácilmente como una sola entidad en una cuenta y una región o en toda la organización de. AWS Organizations

Los paquetes de conformidad se crean generando una plantilla YAML que contiene la lista de reglas administradas o personalizadas y las acciones de corrección de AWS Config . También puede usar AWS Systems Manager documentos (documentos SSM) para almacenar las plantillas de los paquetes de conformidad e implementar directamente los paquetes de conformidad utilizando los nombres de los documentos SSM. AWS Puede implementar la plantilla utilizando la consola de AWS Config o la AWS CLI.

Para empezar rápidamente y evaluar su AWS entorno, utilice una de las plantillas de paquetes de conformidad de ejemplo. También puede crear un archivo YAML del paquete de conformidad desde cero basándose en el paquete de conformidad personalizado.

Temas

- Visualización de los datos de conformidad en el panel de paquetes de conformidad para AWS Config
- Requisito previo para los paquetes de conformidad para AWS Config
- Compatibilidad de la región
- AWS Config Comprobaciones de procesos dentro de un paquete de conformidad para AWS Config
- Plantillas de ejemplo de paquete de conformidad para AWS Config
- Creación de plantillas para paquetes de conformidad personalizados para AWS Config
- Implementación de paquetes de conformidad para AWS Config
- Edición de paquetes de conformidad para AWS Config
- Eliminación de paquetes de conformidad para AWS Config
- Visualización de detalles e información de conformidad en los paquetes de conformidad para AWS Config
- Visualización del cronograma del historial de cumplimiento de los paquetes de conformidad para AWS Config
- Consulta del historial de conformidad de los paquetes de conformidad para AWS Config

- Gestión de paquetes de conformidad para AWS Config todas las cuentas de su organización
- Solución de problemas en paquetes de conformidad para AWS Config

Visualización de los datos de conformidad en el panel de paquetes de conformidad para AWS Config

La página principal de los paquetes de conformidad muestra todos los paquetes de conformidad que tiene actualmente en su Cuenta de AWS. La página también contiene el nombre, el estado de implementación y la puntuación de conformidad de cada paquete de conformidad. La puntuación de conformidad es el porcentaje del número de combinaciones de reglas y recursos conformes en un paquete de conformidad en comparación con el número total de combinaciones posibles de reglas y recursos en el paquete de conformidad.

Puede utilizar este panel para comprender el nivel de conformidad de sus paquetes de conformidad y utilizar la puntuación de conformidad para realizar un seguimiento del progreso de las correcciones, realizar comparaciones entre diferentes conjuntos de requisitos y ver el impacto que un cambio o implementación específicos tienen en un paquete de conformidad.

Navegación por la página principal de los paquetes de conformidad

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Config en https://console.aws.amazon.com/config/home.
2. Navegue a la página de Paquetes de conformidad. Revise los paquetes de conformidad y su puntuación. También puede hacer lo siguiente:
   - Para añadir y configurar un nuevo paquete de conformidad, elija Implementar paquete de conformidad.
   - Para eliminar un paquete de conformidad y sus datos, cambiar los ajustes de configuración o ver detalles adicionales, como la ubicación de entrega o los parámetros, elija un paquete de conformidad y Acciones.

> **Note**
>
> No se puede editar un paquete de conformidad implementado. Puede modificar las demás selecciones en cualquier momento; para ello, elija el nombre del paquete de conformidad y edite en el menú desplegable Acciones.

- Para ver el historial de cambios en el estado de conformidad, elija un paquete de conformidad y Línea de tiempo del paquete de conformidad Para obtener más información, consulte Visualización de la línea de tiempo del historial de conformidad de los paquetes de conformidad.
- Para ver el estado de la implementación, la puntuación de conformidad, la línea de tiempo de la puntuación de conformidad y las reglas de un paquete de conformidad en una vista detallada, elija el paquete de conformidad y Ver.

Requisito previo para los paquetes de conformidad para AWS Config

Antes de implementar el paquete de conformidad, active la grabación. AWS Config

Temas

- Paso 1: Iniciar la AWS Config grabación (obligatorio para todos los paquetes de conformidad)
- Paso 2: requisitos previos adicionales por tipo de paquete de conformidad

Paso 1: Iniciar la AWS Config grabación (obligatorio para todos los paquetes de conformidad)

1. Inicia sesión en la AWS Config consola Consola de administración de AWS y ábrela en https://console.aws.amazon.com/config/casa.
2. Seleccione Configuración en el panel de navegación.
3. Si desea comenzar la grabación, en Recording is off (La grabación está desactivada), elija Turn on (Activar). Cuando se le pregunte, elija Continuar.

Paso 2: requisitos previos adicionales por tipo de paquete de conformidad

A. Requisitos previos para utilizar un paquete de conformidad con corrección

Antes de implementar los paquetes de conformidad mediante plantillas de ejemplo con soluciones, debe crear los recursos adecuados, como la automatización, la asunción de funciones y otros AWS recursos, en función de su objetivo de corrección.

Si tiene un rol de automatización existente que está utilizando para la corrección con documentos SSM, puede proporcionar directamente el ARN de ese rol. Si tiene algún recurso, puede incluirlo en la plantilla.

> **Note**
>
> Al implementar un paquete de conformidad con medidas correctivas en una organización, es necesario especificar el ID de la cuenta de administración de la organización. De lo contrario, durante la implementación del paquete de conformidad organizativo, AWS Config reemplaza automáticamente el ID de la cuenta de administración por el ID de la cuenta del miembro.

AWS Config no admite funciones CloudFormation intrínsecas para la función de ejecución de la automatización o la. `ConfigRuleName` Debe proporcionar el ARN exacto del rol en forma de cadena y debe usar el nombre completo de la regla sin funciones intrínsecas.

Para obtener más información acerca de cómo pasar el ARN exacto, consulte Plantillas de ejemplo de paquete de conformidad para AWS Config. Si utiliza plantillas de muestra, actualice el ID de cuenta y el ID de cuenta de administración de la organización.

B. Requisitos previos para utilizar un paquete de conformidad con una o más reglas personalizadas AWS Config

Antes de implementar un paquete de conformidad con una o más AWS Config reglas personalizadas, cree los recursos adecuados, como la AWS Lambda función y el rol de ejecución correspondiente.

Si ya tiene una AWS Config regla personalizada, puede proporcionar directamente la AWS Lambda función `ARN` of para crear otra instancia de esa regla personalizada como parte del paquete.

Si no tiene una AWS Config regla personalizada existente, puede crear una AWS Lambda función y usar el ARN de la función Lambda. Para obtener más información, consulte AWS Config Reglas personalizadas.

Si su AWS Lambda función está presente en otra Cuenta de AWS, puede crear AWS Config reglas con la autorización de función multicuenta AWS Lambda adecuada. Para obtener más información, consulte la entrada de Cuentas de AWS blog Cómo gestionar de forma centralizada AWS Config las reglas en varias direcciones.

Same account bucket policy

AWS Config Para poder almacenar los artefactos del paquete de conformidad, tendrá que proporcionar un bucket de Amazon S3 y añadir los siguientes permisos. Para obtener más información acerca de los nombres de bucket, consulte Reglas de nomenclatura de buckets.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSConfigConformsBucketPermissionsCheck",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::delivery-bucket-name"
        },
        {
            "Sid": "AWSConfigConformsBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
```

```
}
```

Cross-account bucket policy

AWS Config Para poder almacenar los artefactos del paquete de conformidad, tendrá que proporcionar un bucket de Amazon S3 y añadir los siguientes permisos. Para obtener más información acerca de los nombres de bucket, consulte Reglas de nomenclatura de buckets.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSConfigConformsBucketPermissionsCheck",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
                    "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
        },
        {
            "Sid": "AWSConfigConformsBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/
[optional] prefix/AWSLogs/AccountID/Config/*",
            "Condition": {
                "StringEquals": {
```

```
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        },
        {
            "Sid": " AWSConfigConformsBucketReadAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                ]
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/
[optional] prefix/AWSLogs/AccountID/Config/*"
        }
    ]
}
```

> **Note**
>
> Al implementar paquetes de conformidad entre cuentas, el nombre del bucket de Amazon S3 de entrega debe empezar por `awsconfigconforms`.

C. Requisitos previos de los paquetes de conformidad de la organización

Si la plantilla de entrada tiene una configuración de corrección automática, especifique el ARN del rol de ejecución de automatización de esa corrección en la plantilla. Compruebe que existe un rol con el nombre especificado en todas las cuentas (de administración y miembro) de una organización. Debe crear este rol en todas las cuentas antes de llamar a `PutOrganizationConformancePack`. Puede crear este rol manualmente o usar los AWS CloudFormation conjuntos de pilas para crear este rol en cada cuenta.

Si su plantilla utiliza una función AWS CloudFormation intrínseca `Fn::ImportValue` para importar una variable en particular, entonces esa variable debe definirse como una `Export Value` en todas las cuentas de los miembros de esa organización.

Para ver una AWS Config regla personalizada, consulta el blog Cómo gestionar de forma centralizada AWS Config las reglas en varios Cuentas de AWS blogs para configurar los permisos adecuados.

Política de buckets organizativos:

AWS Config Para poder almacenar los artefactos del paquete de conformidad, tendrá que proporcionar un bucket de Amazon S3 y añadir los siguientes permisos. Para obtener más información acerca de los nombres de bucket, consulte Reglas de nomenclatura de buckets.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/
config-conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/
config-conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

> **Note**
>
> Al implementar paquetes de conformidad en una organización, el nombre del bucket de Amazon S3 de entrega debe empezar por `awsconfigconforms`.

Compatibilidad de la región

Los paquetes de conformidad se admiten en las siguientes regiones:

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Este de EE. UU. (Norte de Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Norte de	us-west-1	config.us-west-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
California)			
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
Asia-Pacífico (Tailandia)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
México (centro)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

En las siguientes regiones se admite la implementación de paquetes de conformidad en las cuentas de los miembros de una AWS organización.

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Este de EE. UU. (Norte de Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Norte de California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
Asia-Pacífico (Tailandia)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
México (centro)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config Comprobaciones de procesos dentro de un paquete de conformidad para AWS Config

Las comprobaciones de procesos son un tipo de AWS Config regla que le permite realizar un seguimiento de las tareas externas e internas que requieren verificación como parte de los paquetes de conformidad. Estas comprobaciones se pueden agregar a un paquete de conformidad existente o a un paquete de conformidad nuevo. Puede realizar un seguimiento de todo el cumplimiento, incluidas las AWS Config duraciones y las comprobaciones manuales, en un solo lugar.

Las comprobaciones de procesos permiten enumerar la conformidad de los requisitos y las acciones en una única ubicación. Estas comprobaciones de procesos ayudan a aumentar la cobertura de los paquetes de conformidad basados en los regímenes de conformidad. Puede ampliar aún más el paquete de conformidad agregando nuevas comprobaciones de procesos que rastreen los procesos y las acciones que requieren verificación y seguimiento manuales. Esto permite que el paquete de conformidad se convierta en la plantilla que proporciona detalles sobre las AWS Config duraciones y los procesos manuales de un régimen de cumplimiento.

Puede realizar un seguimiento y gestionar el cumplimiento de los procesos no asociados a los cambios en la configuración de los recursos dentro de un paquete de conformidad como comprobaciones del proceso. Por ejemplo, puede agregar una verificación del proceso para realizar un seguimiento del requisito de conformidad con el PCI-DSS de almacenar las copias de seguridad

multimedia en una ubicación externa. Evaluará manualmente su conformidad de acuerdo con las directrices del PCI-DSS o según las directrices de su organización.

Disponibilidad regional: las comprobaciones de los procesos con los paquetes de conformidad están disponibles en todos los Regiones de AWS lugares donde estén disponibles los paquetes de AWS Config conformidad. Para obtener más información, consulte Compatibilidad de la región.

Temas

- Ejemplo de plantilla de paquete de conformidad para crear comprobaciones de procesos
- Inclusión de comprobaciones de procesos dentro de un paquete de conformidad
- Cambio del estado de conformidad de una verificación de proceso
- Ver y editar la verificación del proceso (consola)

Ejemplo de plantilla de paquete de conformidad para crear comprobaciones de procesos

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

Consulte dos plantillas de ejemplo, la plantilla Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4 Level 1 y la plantilla Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4 Level 2.

Inclusión de comprobaciones de procesos dentro de un paquete de conformidad

1. Agregue una verificación del proceso en la plantilla del paquete de conformidad. Consulte Ejemplo de plantilla de paquete de conformidad para crear comprobaciones de procesos.

```
Resources:
  ConfigEnabledAllRegions:
    Properties:
      ConfigRuleName: Config-Enabled-All-Regions
      Description: Ensure AWS Config is enabled in all Regions.
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

2. Introduzca el nombre de la verificación del proceso.
3. Introduzca la descripción de la verificación del proceso.
4. Implemente el paquete de conformidad. Para obtener más información, consulte Implementación de paquetes de conformidad para AWS Config.

Cambio del estado de conformidad de una verificación de proceso

Puede cambiar el estado de conformidad de una verificación de proceso mediante la AWS Config consola AWS CLI, el y. APIs

Change Compliance Status for Process Checks (Console)

1. Inicie sesión en la AWS Config consola Consola de administración de AWS y ábrala en https://console.aws.amazon.com/config/casa.
2. Ve a la página de AWS Config reglas.
3. Elija el nombre de la verificación del proceso que especificó en la plantilla junto con el identificador del paquete de conformidad.

> **Note**
>
> Todas las verificaciones del proceso del mismo paquete de conformidad tienen el mismo sufijo.

4. En la página de detalles de la regla, no puede editar la regla, pero puede editar su conformidad. En la sección Conformidad manual, seleccione Editar conformidad.
5. Elija la conformidad adecuada en la lista desplegable.
6. (Opcional) Escriba una descripción del estado de conformidad.
7. Seleccione Save.

Change the Compliance Status for Process Checks (AWS CLI)

Puede actualizar la conformidad de las comprobaciones del proceso dentro de un paquete de conformidad mediante AWS Command Line Interface (AWS CLI).

Para instalarlo AWS CLI en su máquina local, consulte Instalación del AWS CLI en la Guía del AWS CLI usuario.

Si es necesario, escriba `AWS Config ure` para configurar el AWS CLI uso de una AWS región en la que estén disponibles los paquetes de AWS Config conformidad.

1. Abra un símbolo del sistema o una ventana de terminal.
2. Introduzca el siguiente comando para actualizar la conformidad de una verificación de procesos (`ComplianceResourceId` es el `Account ID`) e incluya el nombre de la regla.

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. Pulse Intro para ejecutar el comando.

Change the Compliance Status for Process Checks (API)

Una vez completada la implementación, utilice la API `PutExternalEvaluation` para actualizar las evaluaciones y la conformidad de las comprobaciones del proceso. Para obtener más información, consulte PutExternalEvaluation.

Ver y editar la verificación del proceso (consola)

Solo puede ver las verificaciones del proceso después de agregar un estado de conformidad a las verificaciones del proceso. Elija el paquete de conformidad específico para ver todas las comprobaciones de proceso incluidas en ese paquete de conformidad. Aquí puede ver una lista de las verificaciones de procesos que cumplen y no cumplen con las normas.

Como se trata de una regla vinculada a un servicio, no puede editar la verificación del proceso a través de la página de detalles de la regla.

> **Note**
>
> Sin embargo, puede actualizar la conformidad de la verificación del proceso seleccionando Editar conformidad y seleccionando el valor adecuado entre Conforme, No conforme o No aplicable.

Puede editar o eliminar una verificación de proceso del paquete de conformidad en el que haya agregado las verificaciones de proceso.

Plantillas de ejemplo de paquete de conformidad para AWS Config

Estas son algunas plantillas de YAML de los paquetes de conformidad que puede ver en la consola de AWS Config. En la plantilla de paquetes de conformidad, puede utilizar una o varias acciones de corrección y reglas de AWS Config. Las reglas de AWS Config enumeradas en el paquete de conformidad pueden ser reglas administradas de AWS Config o reglas personalizadas de AWS Config. Puedes descargar todas las plantillas del paquete de conformidad desde GitHub.

> **Important**
>
> Los paquetes de conformidad proporcionan un marco de conformidad de propósito general para ayudarle a crear comprobaciones de control de seguridad, operativas o de optimización de costos mediante reglas administradas o personalizadas de AWS Config y acciones de corrección de AWS Config. Las plantillas de ejemplo del paquete de conformidad de AWS tienen la intención de ayudarle a crear sus propios paquetes de conformidad con reglas, parámetros de entrada y acciones de corrección diferentes o adicionales que se adapten a su entorno. Las plantillas de ejemplo, incluidas las relacionadas con las normas de conformidad y los parámetros de referencia del sector, no están diseñadas para garantizar

la conformidad de una norma de gobierno específica. No pueden reemplazar los esfuerzos internos ni garantizar que superará una evaluación de conformidad.

> **Note**
>
> Se recomienda revisar las reglas disponibles en la región en la que implemente un paquete de conformidad (Lista de reglas de AWS Config administradas por disponibilidad regional) y que modifique la plantilla para incluir las reglas que aún no estén disponibles en esa región antes de implementarlas.

Temas

- AWS Paquete de conformidad con las barandillas Control Tower Detective
- Prácticas recomendadas de ciberresiliencia para Amazon S3, Amazon EBS y Amazon DynamoDB
- Prácticas operativas recomendadas para cargas de trabajo de material de ABS CCIG 2.0
- Prácticas operativas recomendadas para cargas de trabajo estándar de ABS CCIG 2.0
- Prácticas operativas recomendadas para ACSC Essential 8
- Prácticas operativas recomendadas para ACSC ISM: parte 1
- Prácticas operativas recomendadas para ACSC ISM: parte 2
- Prácticas operativas recomendadas para IA y ML
- Prácticas operativas recomendadas para Amazon API Gateway
- Mejores prácticas operativas para Amazon CloudWatch
- Prácticas operativas recomendadas para Amazon DynamoDB
- Prácticas operativas recomendadas para Amazon S3
- Prácticas operativas recomendadas para APRA CPG 234
- Prácticas operativas recomendadas para la gestión de activos
- Mejores prácticas operativas para AWS Backup
- Prácticas operativas recomendadas para AWS Identity and Access Management
- Mejores prácticas operativas para el pilar de confiabilidad de AWS un marco de trabajo bien diseñado
- Mejores prácticas operativas para el pilar de seguridad de AWS Well-Architected Framework
- Prácticas operativas recomendadas para BCP y DR

- Mejores prácticas operativas para BNM T RMi
- Prácticas operativas recomendadas para el Perfil medio de control de la nube del Centro Canadiense de Ciberseguridad (CCCS)
- Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4 Level 1
- Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4 Level 2
- Mejores prácticas operativas para los controles de seguridad críticos de CIS v8 IG1
- Mejores prácticas operativas para los controles de seguridad críticos de CIS v8 IG2
- Mejores prácticas operativas para los controles de seguridad críticos de CIS v8 IG3
- Prácticas operativas recomendadas para los 20 principales controles del CIS
- Prácticas operativas recomendadas para CISA Cyber Essentials
- Prácticas operativas recomendadas para los Servicios de Información de la Justicia Criminal (CJIS, por sus siglas en inglés)
- Prácticas operativas recomendadas para la CMMC 2.0 de nivel 1
- Prácticas operativas recomendadas para la CMMC 2.0 de nivel 2
- Prácticas operativas recomendadas para servicios de computación
- Prácticas operativas recomendadas para la resiliencia de datos
- Prácticas operativas recomendadas para servicios de bases de datos
- Prácticas operativas recomendadas para lagos de datos y servicios de análisis
- Mejores prácticas operativas para DevOps
- Prácticas operativas recomendadas para EC2
- Prácticas operativas recomendadas para el cifrado y la administración de claves
- Prácticas operativas recomendadas para la guía de ciberseguridad para pymes de la ENISA
- Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Bajo
- Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Medio
- Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Alto
- Prácticas operativas recomendadas para la FDA Título 21 CFR Parte 11
- Prácticas operativas recomendadas para el FedRAMP (bajo)
- Prácticas operativas recomendadas para FedRAMP (moderadas)
- Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 1)
- Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 2)
- Prácticas operativas recomendadas para FFIEC

- Catálogo de criterios de cumplimiento de las prácticas recomendadas operativas para la computación en la nube en Alemania (C5)
- Prácticas recomendadas operativas para la Ley Gramm Leach Bliley (GLBA)
- Prácticas operativas recomendadas para el anexo 11 de la UE de GxP
- Prácticas operativas recomendadas para la seguridad de la HIPAA
- Prácticas operativas recomendadas para IRS 1075
- Prácticas operativas recomendadas para K-ISMS
- Prácticas operativas recomendadas para el equilibrado de carga
- Prácticas operativas recomendadas para el registro
- Prácticas operativas recomendadas para servicios de administración y gobernanza
- Prácticas operativas recomendadas para MAS Notice 655
- Prácticas operativas recomendadas para MAS TRMG
- Prácticas operativas recomendadas para el monitoreo
- Prácticas operativas recomendadas para NBC TRMG
- Prácticas operativas recomendadas para NERC CIP BCSI
- Prácticas operativas recomendadas para los NCSC Cloud Security Principles
- Prácticas operativas recomendadas para el NCSC Cyber Assesment Framework
- Prácticas operativas recomendadas para redes y servicios de entrega de contenido
- Prácticas operativas recomendadas para el NIST 800-53 rev 4
- Prácticas operativas recomendadas para el NIST 800-53 rev 5
- Prácticas operativas recomendadas para NIST 800 171
- Prácticas operativas recomendadas para NIST 800 172
- Prácticas operativas recomendadas para NIST 800 181
- Prácticas operativas recomendadas para NIST 1800 25
- Prácticas operativas recomendadas para el NIST CSF
- Prácticas operativas recomendadas para el NIST Privacy Framework v1.0
- Prácticas operativas recomendadas para NYDFS 23
- Prácticas operativas recomendadas para NZISM 3.8
- Prácticas operativas recomendadas para el PCI DSS 3.2.1
- Prácticas operativas recomendadas para el PCI DSS 4.0 (excluye los tipos de recursos globales)

- Prácticas operativas recomendadas para el PCI DSS 4.0 (incluye los tipos de recursos globales)
- Prácticas operativas recomendadas para recursos de acceso público
- Mejores prácticas operativas para el marco de ciberseguridad del RBI para UCBs
- Prácticas operativas recomendadas para RBI MD-ITF
- Prácticas operativas recomendadas para los servicios de seguridad, identidad y conformidad
- Prácticas operativas recomendadas para soluciones sin servidor
- Prácticas operativas recomendadas para servicios de almacenamiento
- Prácticas operativas recomendadas para el SWIFT CSP
- Prácticas de seguridad recomendadas para Amazon Elastic Container Service (Amazon ECS)
- Prácticas de seguridad recomendadas para Amazon Elastic File System (Amazon EFS)
- Prácticas de seguridad recomendadas para Amazon Elastic Kubernetes Service (Amazon EKS)
- Mejores prácticas de seguridad para Amazon CloudFront
- Mejores prácticas de seguridad para Amazon OpenSearch Service
- Prácticas de seguridad recomendadas para Amazon Redshift
- Prácticas de seguridad recomendadas para Amazon Relational Database Service (Amazon RDS)
- Mejores prácticas de seguridad para AWS Auto Scaling
- Mejores prácticas de seguridad para AWS CloudTrail
- Mejores prácticas de seguridad para AWS CodeBuild
- Prácticas recomendadas de seguridad para Amazon ECR
- Mejores prácticas de seguridad para AWS Lambda
- Mejores prácticas de seguridad para AWS Network Firewall
- Prácticas de seguridad recomendadas para Amazon SageMaker AI
- Mejores prácticas de seguridad para AWS Secrets Manager
- Mejores prácticas de seguridad para AWS WAF
- Plantillas de ejemplo con acción de corrección

AWS Paquete de conformidad con las barandillas Control Tower Detective

Este paquete de conformidad contiene AWS Config reglas basadas en las barandillas de Detective AWS de la Torre de Control. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de AWS Config reglas administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: AWS Control Tower Detective Guardrails Conformance Pack.

Prácticas recomendadas de ciberresiliencia para Amazon S3, Amazon EBS y Amazon DynamoDB

Este paquete de conformidad contiene AWS Config reglas basadas en las prácticas recomendadas de ciberresiliencia para Amazon S3, Amazon EBS y Amazon DynamoDB. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas administradas. AWS Config

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas de resiliencia cibernética para Amazon S3, Amazon EBS y Amazon DynamoDB.

Prácticas operativas recomendadas para cargas de trabajo de material de ABS CCIG 2.0

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre la Guía de implementación de computación en nube 2.0 de ABS (Material Workloads) y las reglas de configuración AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de la Guía de implementación de computación en nube de ABS. Un control de la guía de implementación de computación en la nube de ABS puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 2: cargas de trabajo materiale s	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
sección 4a-govern-the-cloud: 2: cargas de trabajo materiale s	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
sección 4:2: cargas de trabajo estándar a-govern-the-cloud	account-part-of-organizations	La administración centraliz ada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centraliz

ID de control	AWS Regla de configuración	Directrices
		ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	cloudtrail-s3-dataevents-en abled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
sección 4 -2: cargas a-govern-the-cloud de trabajo estándar	cloudtrail-security-trail-enabled	Esta regla ayuda a garantiza r el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico o de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4:3: cargas de trabajo materiales a-govern-the-cloud	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de actividad que puede soportar cada mesa. read/write DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentag e de cuenta (Config Default: 80). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 3: cargas de trabajo materiales	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.
sección 4 -3: cargas a-govern-the-cloud de trabajo estándar	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 3: cargas de trabajo estándar	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
sección 4 -3: cargas a-govern-the-cloud de trabajo estándar	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminaci ón al finalizar una instancia . Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3a-govern-the-cloud: cargas de trabajo estándar	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear las no utilizadas en su entorno. EIPs
sección 4a-govern-the-cloud: 3: cargas de trabajo estándar	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.
sección 4b-design-and-secure: cargas de trabajo estándar en la nube	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo estándar en la nube 1 b-design-and-secure	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secu re: la nube: 1 carga de trabajo estándar	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
b-design-and-securesección 4: la nube, 1: cargas de trabajo estándar	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
sección 4b-design-and-secure: cargas de trabajo estándar en la nube 1	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo estándar en la nube b-design-and-secure	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y el estándar fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. AWS Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: cargas de trabajo estándar en la nube 1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: cargas de trabajo estándar en la nube b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: cargas de trabajo estándar en la nube	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube, 1 carga de trabajo estándar	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 1: cargas de trabajo estándar	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
sección 4: la nube, 1 carga de trabajo estándar b-design-and-secure	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: la nube, 1 carga de trabajo estándar b-design-and-secure	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: la nube: 1 carga de trabajo estándar	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuac ión, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: cargas de trabajo estándar en la nube 1	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 1 carga de trabajo estándar	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4b-design-and-secure: la nube, 1: cargas de trabajo estándar	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: cargas de trabajo estándar en la nube	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: la nube, 1 carga de trabajo estándar	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	subnet-auto-assign-public-ip-deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
sección 4: las cargas de trabajo estándar de la nube 2 b-design-and-secure	cloudtrail-security-trail-enabled	Esta regla ayuda a garantiza r el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 2 cargas de trabajo estándar	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 2	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 2	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 2	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube, 3 cargas de trabajo materiales	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
b-design-and-securesección 4: la nube, las 3 cargas de trabajo materiales	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 3 cargas de trabajo materiales b-design-and-secure	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
sección 4: las cargas de trabajo materiales b-design-and-secure de la nube, 3	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las cargas de trabajo de la nube, 3 materiales	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibi lidad y durabilidad de las instancias de bases de datos. Cuando aprovisio na una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutaci ón por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo materiales b-design-and-secure de la nube, 3	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las cargas de trabajo de la nube, 3 materiales	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 3	autoscaling-group-elb-healt hcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibi lidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 3	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
b-design-and-securesección 4: las cargas de trabajo estándar de la nube, las 3	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 3	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
sección 4: las cargas de trabajo estándar de la nube (3) b-design-and-secure	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 3	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 3	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 3	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 3	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.
b-design-and-securesección 4: la nube, 4 cargas de trabajo materiales	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: La nube, 4 cargas de trabajo materiales b-design-and-secure	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
sección 4b-design-and-secure: La nube, 4 cargas de trabajo materiales	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo de la nube, 4 materiale s b-design-and-secure	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: La nube, 4 cargas de trabajo materiales	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: La nube, 4 cargas de trabajo materiales	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 4 cargas de trabajo materiales	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube, 4 cargas de trabajo materiales	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 4 cargas de trabajo materiales	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
sección 4: la nube, 4 cargas de trabajo materiales b-design-and-secure	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: La nube, 4 cargas de trabajo materiales	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.
sección 4: las cargas de trabajo de la nube, 4 materiale s b-design-and-secure	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: La nube, 4 cargas de trabajo materiales b-design-and-secure	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
sección 4: la nube, 4 cargas de trabajo materiales b-design-and-secure	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4: La nube, 4 cargas de trabajo materiales b-design-and-secure	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: la nube, 4 cargas de trabajo materiales	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 4 cargas de trabajo materiales	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secu re: las cargas de trabajo de la nube, 4 materiales	sagemaker-notebook-no-direc t-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 4 cargas de trabajo materiales	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
b-design-and-securesección 4: La nube, 4 cargas de trabajo materiales	vpc-default-security-group-cerrada	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 4 cargas de trabajo materiales	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 4 cargas de trabajo materiales	vpc-vpn-2-tunnels-up	Se pueden implementar túneles VPN redundantes Site-to-Site para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.
sección 4b-design-and-secure: La nube, 4 cargas de trabajo materiales	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: La nube, 4 cargas de trabajo materiales	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
sección 4b-design-and-secu re: Las cargas de trabajo estándar de la nube, 4	autoscaling-launch-config-p ublic-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidore s.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 4 b-design-and-secure	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secu re: Las cargas de trabajo estándar de la nube, 4	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 4	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube, 4	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube, 4	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y el estándar fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. AWS Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: Las cargas de trabajo estándar de la nube, 4 b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube, 4	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube y las 4 b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube, 4	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, las 4	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: las cargas de trabajo estándar de la nube, 4	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube y las 4 b-design-and-secure	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
sección 4: las cargas de trabajo estándar de la nube y las 4 b-design-and-secure	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 4	sagemaker-notebook-no-direc t-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	vpc-default-security-group-cerrada	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	vpc-vpn-2-tunnels-up	Se pueden implementar túneles VPN redundantes Site-to-Site para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, las 4	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
sección 4: la nube, 5 cargas de trabajo materiales b-design-and-secure	cmk-backing-key-rotation-ha bilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
sección 4b-design-and-secu re: las cargas de trabajo de la nube, 5 materiales	iam-root-access-key-comprob ar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorpora r el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 5 cargas de trabajo materiales b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
sección 4: las cargas de trabajo de la b-design-and-secure nube, 5 materiales	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 5 cargas de trabajo materiales b-design-and-secure	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 5	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 5	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, las 5	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 5 b-design-and-secure	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 5 b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 5	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
sección 4b-design-and-secure: la nube, seis cargas de trabajo materiales	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 6 cargas de trabajo materiales	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4: La nube, seis cargas de trabajo materiales b-design-and-secure	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4: La nube, seis cargas de trabajo materiales b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo de la nube, 6 materiales b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo de la b-design-and-secure nube con 6 materiales	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
sección 4b-design-and-secu re: las seis cargas de trabajo estándar de la nube	alb-http-drop-invalid-habilitado para encabezados	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 6	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
sección 4b-design-and-secu re: la nube, las 6 cargas de trabajo estándar	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
b-design-and-securesección 4: la nube, las 6 cargas de trabajo estándar	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 6	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
sección 4: la nube, las 6 cargas de trabajo estándar b-design-and-secure	elb v2- acm-certificate-re quired	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
sección 4: la nube, las 6 cargas de trabajo estándar b-design-and-secure	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitad o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
b-design-and-securesección 4: las seis cargas de trabajo estándar de la nube	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 6	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 6	sagemaker-endpoint-configuration-kms-configurado mediante clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
sección 4b-design-and-secure: la nube, las 6 cargas de trabajo estándar	sagemaker-notebook-instance-kms-configurado mediante clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, las 6 cargas de trabajo estándar	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: las seis cargas de trabajo estándar de la nube	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo de la nube, 8 materiales	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
sección 4: la nube, 8 cargas de trabajo materiales b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo de 8 b-design-and-secure materiales de la nube	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: la nube, 8 cargas de trabajo materiales b-design-and-secure	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 8 cargas de trabajo materiales	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 8	account-part-of-organizations	La administración centraliz ada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centraliz ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 8	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 8 cargas de trabajo estándar	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 8	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 8 b-design-and-secure	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, las 8 cargas de trabajo estándar b-design-and-secure	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 8 b-design-and-secure	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integrada s. Las políticas administr adas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y el estándar fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. AWS Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 8	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegi o y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 8 b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 8	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 8 cargas de trabajo estándar b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo estándar de la nube, 8 b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 8	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: la nube, 8 cargas de trabajo estándar b-design-and-secure	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: la nube, 9 cargas de trabajo materiales	cloudtrail-security-trail-enabled	Esta regla ayuda a garantiza r el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 9 cargas de trabajo materiales	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
sección 4b-design-and-secure: la nube, 9 cargas de trabajo materiales	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 9 cargas de trabajo materiales b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
sección 4: la nube, 9 b-design-and-secure cargas de trabajo materiales	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 9 cargas de trabajo materiales b-design-and-secure	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: la nube, 9 cargas de trabajo materiales	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de administración y las llamadas a la API. AWS Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
sección 4b-design-and-secure: Las cargas de trabajo estándar de la nube 9	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 9 b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 9	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 9 b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo estándar de la nube 9 b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 9	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: las cargas de trabajo estándar de la nube 9 b-design-and-secure	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 10 cargas de trabajo materiales b-design-and-secure	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
sección 4: las cargas de trabajo de los 10 materiales de la nube b-design-and-secure	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo de los 10 materiales de la nube	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: la nube, 10 cargas de trabajo materiales	ec2- -manager instance-managed-by-systems	Es posible realizar un inventari o de las plataformas y aplicaciones de software de la organización mediante la administración de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configura ciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo materiales de la nube	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secu re: las 10 cargas de trabajo materiales de la nube	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secu re: las 10 cargas de trabajo materiales de la nube	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las 10 cargas de trabajo materiales de la nube	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y el estándar fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. AWS Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo materiales de la nube	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo materiales de la nube b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
sección 4: las cargas de trabajo de los b-design-and-secure 10 materiales de la nube	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: las 10 cargas de trabajo materiales de la nube	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
sección 4: las 10 cargas de trabajo materiales de la nube b-design-and-secure	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo materiales de la nube	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: las 10 cargas de trabajo materiales de la nube b-design-and-secure	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo materiales de la nube b-design-and-secure	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
sección 4: las 10 cargas de trabajo materiales de la nube b-design-and-secure	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo materiales de la nube b-design-and-secure	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
sección 4b-design-and-secu re: las 10 cargas de trabajo materiales de la nube	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuac ión, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo materiales de la nube	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 10 cargas de trabajo materiales	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: la nube, 10 cargas de trabajo materiales	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 10 cargas de trabajo materiales	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo de los 10 materiales de la nube	sagemaker-notebook-no-direc t-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: la nube, las 10 cargas de trabajo materiales	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
b-design-and-securesección 4: las 10 cargas de trabajo materiales de la nube	vpc-default-security-group-cerrada	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las 10 cargas de trabajo materiales de la nube	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 10 cargas de trabajo materiales	vpc-vpn-2-tunnels-up	Se pueden implementar túneles VPN redundantes Site-to-Site para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.
sección 4b-design-and-secu re: las 10 cargas de trabajo materiales de la nube	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo materiales de la nube	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.
sección 4: las 10 cargas de trabajo b-design-and-secure estándar de la nube	autoscaling-launch-config-p ublic-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidore s.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: las 10 cargas de trabajo estándar de la nube	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las 10 cargas de trabajo estándar de la nube	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
sección 4: las 10 cargas de trabajo b-design-and-secure estándar de la nube	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: las 10 cargas de trabajo estándar de la nube	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las 10 cargas de trabajo estándar de la nube	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las 10 cargas de trabajo estándar de la nube	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	sagemaker-notebook-no-direc t-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
b-design-and-securesección 4: las 10 cargas de trabajo estándar de la nube	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	vpc-sg-open-only-to-authori zed-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/ 0), se puede controlar el acceso remoto a los sistemas internos.
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	s3- -prohibido bucket-level- public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las 10 cargas de trabajo estándar de la nube	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
sección 4: las 11 cargas de trabajo materiales de la nube b-design-and-secure	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
sección 4b-design-and-secure: las 11 cargas de trabajo materiales de la nube	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure materiales de la nube	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
sección 4b-design-and-secure: la nube, 11 cargas de trabajo materiales	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo materiales de la nube 11	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
sección 4b-design-and-secure: las cargas de trabajo materiales de la nube 11	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 11 cargas de trabajo materiales	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
sección 4: las cargas de trabajo b-design-and-secure materiales de la nube	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 11 cargas de trabajo materiales de la nube	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.
sección 4b-design-and-secure: la nube, 11 cargas de trabajo materiales	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure materiales de la nube	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: las cargas de trabajo materiale s de la nube 11	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo materiale s de la nube 11	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
sección 4: la nube, 11 cargas de trabajo materiales b-design-and-secure	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure materiales de la nube	wafv2-logging-enabled	Para facilitar el registro y la supervisión de su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personale s ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild . AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credencia les de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
b-design-and-securesección 4: la nube, 12 cargas de trabajo estándar	dynamodb-table-encrypted-km s	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube, 12 cargas de trabajo estándar	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 12 cargas de trabajo estándar b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: la nube, 12 cargas de trabajo estándar b-design-and-secure	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitad o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
b-design-and-securesección 4: la nube, 12 cargas de trabajo estándar	habilitado para s3 bucket-se rver-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	sagemaker-endpoint-configuration-kms-configurado mediante clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	sagemaker-notebook-instance-kms-configurado mediante clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo materiales	cloudtrail-s3-dataevents-en abled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 b-design-and-secure cargas de trabajo materiales	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas, ya que comprueba la habilitación de varios ajustes AWS CloudTrail. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo materiales	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo materiales	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo importantes	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo materiales	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.
sección 4: la nube, 14 b-design-and-secure cargas de trabajo materiales	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 cargas de trabajo materiales b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
sección 4b-design-and-secure: La nube, 14 cargas de trabajo importantes	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 cargas de trabajo materiales b-design-and-secure	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatiz adas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantán ea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
sección 4: la nube, 14 b-design-and-secure cargas de trabajo materiales	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 cargas de trabajo estándar b-design-and-secure	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas, ya que comprueba la habilitación de varios ajustes AWS CloudTrail. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	cloud-trail-cloud-watch-habilitada para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
b-design-and-securesección 4: la nube, 14 cargas de trabajo estándar	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: la nube, 14 cargas de trabajo estándar b-design-and-secure	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube, 14 cargas de trabajo estándar	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 cargas de trabajo estándar b-design-and-secure	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
sección 4: la nube, 14 cargas de trabajo estándar b-design-and-secure	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	wafv2-logging-enabled	Para facilitar el registro y la supervisión de su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo materiales	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo de 15 b-design-and-secure materiales en la nube	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 15 cargas de trabajo materiales b-design-and-secure	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 15 cargas de trabajo materiales b-design-and-secure	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
sección 4: la nube, 15 b-design-and-secure cargas de trabajo estándar	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube: 15 cargas de trabajo estándar	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
b-design-and-securesección 4: la nube: 15 cargas de trabajo estándar	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
sección 4: la nube, 15 b-design-and-secure cargas de trabajo estándar	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 15 b-design-and-secure cargas de trabajo estándar	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
sección 4b-design-and-secure: 15 cargas de trabajo estándar en la nube	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 15 cargas de trabajo estándar b-design-and-secure	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
sección 4: la nube, 15 cargas de trabajo estándar b-design-and-secure	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 15 b-design-and-secure cargas de trabajo estándar	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
sección 4:15 cargas de trabajo estándar en la nube b-design-and-secure	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
sección 4 -1c-run-the-cloud: cargas de trabajo estándar	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de administración y las llamadas a la API. AWS Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 2: cargas de trabajo materiales	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
sección 4c-run-the-cloud: 2: cargas de trabajo materiales	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4 -2c-run-the-cloud: cargas de trabajo estándar	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico o de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.
sección 4c-run-the-cloud: 2: cargas de trabajo estándar	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 2: cargas de trabajo estándar	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.
sección 4:2: cargas de trabajo estándar c-run-the-cloud	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integrada s. Las políticas administr adas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 2: cargas de trabajo estándar	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4:2: cargas de trabajo estándar c-run-the-cloud	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4 -2: cargas c-run-the-cloud de trabajo estándar	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
sección 4:2: cargas de trabajo estándar c-run-the-cloud	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4:2: cargas de trabajo estándar c-run-the-cloud	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4c-run-the-cloud: 2: cargas de trabajo estándar	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4:3: cargas de trabajo estándar c-run-the-cloud	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
sección 4 -3c-run-the-cloud: cargas de trabajo estándar	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de administración y las llamadas a la API. AWS Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	AWS Regla de configuración	Directrices
c-run-the-cloudsección 4:3: cargas de trabajo estándar	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	multi-region-cloudtrail-enabled	AWS CloudTrail registra AWS las acciones de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
c-run-the-cloudsección 4:3: cargas de trabajo estándar	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3c-run-the-cloud: cargas de trabajo estándar	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
sección 4:3: cargas de trabajo estándar c-run-the-cloud	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
sección 4c-run-the-cloud: 4 cargas de trabajo estándar	response-plan-exists-mainta ined (verificación del proceso)	Asegúrese de que los planes de respuesta ante incidente s se establezcan, actualice n y distribuyan al personal responsable.
sección 4c-run-the-cloud: 4: cargas de trabajo materiales	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4:4: cargas de trabajo materiales c-run-the-cloud	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
sección 4c-run-the-cloud: 4: cargas de trabajo materiales	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 4: cargas de trabajo materiales	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4:5: cargas de trabajo estándar c-run-the-cloud	autoscaling-group-elb-healthcheck- obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.
sección 4 -5c-run-the-cloud: cargas de trabajo estándar	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 5: cargas de trabajo estándar	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	AWS Regla de configuración	Directrices
sección 4:5: cargas de trabajo estándar c-run-the-cloud	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de actividad que puede soportar cada mesa. read/write DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentag e de cuenta (Config Default: 80). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 5: cargas de trabajo estándar	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
sección 4 -5c-run-the-cloud: cargas de trabajo estándar	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	AWS Regla de configuración	Directrices
sección 4 -5: cargas c-run-the-cloud de trabajo estándar	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	AWS Regla de configuración	Directrices
sección 4 -5: cargas c-run-the-cloud de trabajo estándar	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	AWS Regla de configuración	Directrices
c-run-the-cloudsección 4:6 cargas de trabajo materiales	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
sección 4c-run-the-cloud: 6 cargas de trabajo materiales	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4 -6-cargas de trabajo materiales c-run-the-cloud	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
sección 4c-run-the-cloud: 6 cargas de trabajo materiales	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 6: cargas de trabajo materiales	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4:6 cargas de trabajo estándar c-run-the-cloud	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
sección 4c-run-the-cloud: 6 cargas de trabajo estándar	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 6 cargas de trabajo estándar	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4:6 cargas de trabajo estándar c-run-the-cloud	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para cargas de trabajo con materiales ABS CCIG 2.0.

Prácticas operativas recomendadas para cargas de trabajo estándar de ABS CCIG 2.0

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre la Guía de implementación de computación en nube 2.0 de ABS: cargas de trabajo estándar y las reglas de configuración AWS administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de la Guía de implementación de computación en nube de ABS. Un control de la guía de implementación de computación en la nube de ABS puede estar relacionado con varias reglas de

Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
sección 4 -2: cargas a-govern-the-cloud de trabajo estándar	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la

ID de control	AWS Regla de configuración	Directrices
		validación de registros y la habilitación AWS CloudTrail en varias regiones.
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 2: cargas de trabajo estándar	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4:3: cargas de trabajo estándar a-govern-the-cloud	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
sección 4a-govern-the-cloud: 3: cargas de trabajo estándar	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3: cargas a-govern-the-cloud de trabajo estándar	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.
sección 4 -3a-govern-the-cloud: cargas de trabajo estándar	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear las no utilizadas en su entorno. EIPs

ID de control	AWS Regla de configuración	Directrices
sección 4a-govern-the-cloud: 3: cargas de trabajo estándar	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.
sección 4b-design-and-secure: cargas de trabajo estándar en la nube 1	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
sección 4: cargas de trabajo estándar en la nube 1 b-design-and-secure	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube: 1 carga de trabajo estándar	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
b-design-and-securesección 4: las cargas de trabajo estándar de la nube 1	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: cargas de trabajo estándar en la nube 1	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo estándar en la nube b-design-and-secure	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomiend a utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y el estándar fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. AWS Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: cargas de trabajo estándar en la nube 1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegi o y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: cargas de trabajo estándar en la nube b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: cargas de trabajo estándar en la nube	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube, 1 carga de trabajo estándar	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 1: cargas de trabajo estándar	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
sección 4: la nube, 1 carga de trabajo estándar b-design-and-secure	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: la nube, 1 carga de trabajo estándar b-design-and-secure	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
sección 4: las cargas de trabajo estándar de la nube 1 b-design-and-secure	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: la nube: 1 carga de trabajo estándar	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuac ión, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: cargas de trabajo estándar en la nube 1	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 1 carga de trabajo estándar	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4b-design-and-secure: la nube 1: cargas de trabajo estándar	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: cargas de trabajo estándar en la nube	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 1 carga de trabajo estándar	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	AWS Regla de configuración	Directrices
sección 4: cargas de trabajo b-design-and-secure estándar de la nube 1	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearch Permite un control de acceso al dominio basado en funciones, así como una seguridad a nivel de índices, documentos y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearch
b-design-and-securesección 4: las cargas de trabajo estándar de la nube 1	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 1	subnet-auto-assign-public-ip-deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
sección 4: las cargas de trabajo estándar de la nube 2 b-design-and-secure	cloudtrail-security-trail-enabled	Esta regla ayuda a garantiza r el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 2	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 2	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 2	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 2	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: las cargas de trabajo estándar de la nube 3	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 3	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: las cargas de trabajo estándar de la nube, las 3	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 3	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube (3) b-design-and-secure	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 3	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 3	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 3	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 3	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.
b-design-and-securesección 4: las cargas de trabajo estándar de la nube, 4	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
sección 4b-design-and-secu re: Las cargas de trabajo estándar de la nube, 4	autoscaling-launch-config-p ublic-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidore s.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 4 b-design-and-secure	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secu re: Las cargas de trabajo estándar de la nube, 4	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 4	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube, 4	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearc h Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube, 4	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomiend a utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y el estándar fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. AWS Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegi o y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube, 4	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube y las 4 b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube, 4	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, las 4	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: las cargas de trabajo estándar de la nube, 4	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
sección 4: las cargas de trabajo estándar de la nube, las 4 b-design-and-secure	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: Las cargas de trabajo estándar de la nube, 4 b-design-and-secure	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
sección 4: las cargas de trabajo estándar de la nube, 4 b-design-and-secure	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube y las 4	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 4	sagemaker-notebook-no-direc t-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	vpc-default-security-group-cerrada	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	vpc-vpn-2-tunnels-up	Se pueden implementar túneles VPN redundantes Site-to-Site para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 4	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
sección 4: las cargas de trabajo estándar de la nube, las 5 b-design-and-secure	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 5	cmk-backing-key-rotation-ha bilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, las 5	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 5 b-design-and-secure	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomiend a utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 5 b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegi os de los necesarios para completar una tarea puede infringir el principio de privilegi o mínimo y la separación de funciones.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 5	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
sección 4b-design-and-secu re: las seis cargas de trabajo estándar de la nube	alb-http-drop-invalid-habilitado para encabezados	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4: las seis cargas de trabajo estándar de la nube b-design-and-secure	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 6	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
sección 4b-design-and-secu re: la nube, las 6 cargas de trabajo estándar	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
b-design-and-securesección 4: las seis cargas de trabajo estándar de la nube	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 6	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
sección 4: la nube, las 6 cargas de trabajo estándar b-design-and-secure	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, las 6 cargas de trabajo estándar b-design-and-secure	elb v2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 6 b-design-and-secure	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
sección 4: la nube, las 6 cargas de trabajo estándar b-design-and-secure	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
b-design-and-securesección 4: las seis cargas de trabajo estándar de la nube	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 6	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 6	sagemaker-endpoint-configuration-kms-configurado mediante clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
sección 4b-design-and-secure: la nube, las 6 cargas de trabajo estándar	sagemaker-notebook-instance-kms-configurado mediante clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, las 6 cargas de trabajo estándar	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: las seis cargas de trabajo estándar de la nube	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 8	account-part-of-organizations	La administración centraliz ada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centraliz ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 8	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 8 b-design-and-secure	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, las 8 cargas de trabajo estándar b-design-and-secure	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomiend a utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 8 b-design-and-secure	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 8	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y el estándar fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. AWS Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 8	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegi o y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 8 b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 8	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube, 8 b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo estándar de la nube, 8 b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringi r el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autentica ción multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protecció n además de un nombre de usuario y una contraseñ a. Reduzca los incidente s de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 8	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, las 8 cargas de trabajo estándar	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: las cargas de trabajo estándar de la nube, 8 b-design-and-secure	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube, 8	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de administración y las llamadas a la API. AWS Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: las cargas de trabajo estándar de la nube 9 b-design-and-secure	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 9	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
sección 4: las cargas de trabajo estándar de la nube b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las cargas de trabajo estándar de la nube 9 b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
sección 4: las cargas de trabajo b-design-and-secure estándar de la nube 9	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: las cargas de trabajo estándar de la nube 9 b-design-and-secure	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las cargas de trabajo estándar de la nube 9	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.
sección 4: las 10 cargas de trabajo b-design-and-secure estándar de la nube	autoscaling-launch-config-p ublic-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidore s.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	iam-no-inline-policy-compro bar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegi o y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo b-design-and-secure estándar de la nube	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: las 10 cargas de trabajo estándar de la nube	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las 10 cargas de trabajo estándar de la nube	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: las 10 cargas de trabajo estándar de la nube	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4: las 10 cargas de trabajo estándar de la nube b-design-and-secure	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: las 10 cargas de trabajo estándar de la nube	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
sección 4b-design-and-secure: las 10 cargas de trabajo estándar de la nube	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	sagemaker-notebook-no-direc t-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
b-design-and-securesección 4: las 10 cargas de trabajo estándar de la nube	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	vpc-sg-open-only-to-authori zed-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/ 0), se puede controlar el acceso remoto a los sistemas internos.
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	s3- -prohibido bucket-level- public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secu re: las 10 cargas de trabajo estándar de la nube	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
sección 4: la nube, 12 cargas de trabajo estándar b-design-and-secure	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personale s ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personale s o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
b-design-and-securesección 4: la nube, 12 cargas de trabajo estándar	dynamodb-table-encrypted-km s	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube, 12 cargas de trabajo estándar	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 12 cargas de trabajo estándar b-design-and-secure	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4: la nube, 12 cargas de trabajo estándar b-design-and-secure	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitad o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 12 b-design-and-secure cargas de trabajo estándar	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
b-design-and-securesección 4: la nube, 12 cargas de trabajo estándar	habilitado para s3 bucket-se rver-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	sagemaker-endpoint-configuration-kms-configurado mediante clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	sagemaker-notebook-instance-kms-configurado mediante clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 12 cargas de trabajo estándar	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	api-gw-execution-logging-ha bilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	cloudtrail-s3-dataevents-en abled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas, ya que comprueba la habilitación de varios ajustes AWS CloudTrail. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube, 14 cargas de trabajo estándar	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	elasticsearch-logs-to-cloud watch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 cargas de trabajo estándar b-design-and-secure	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube, 14 cargas de trabajo estándar	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 cargas de trabajo estándar b-design-and-secure	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
sección 4: la nube, 14 cargas de trabajo estándar b-design-and-secure	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 14 b-design-and-secure cargas de trabajo estándar	wafv2-logging-enabled	Para facilitar el registro y la supervisión de su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
sección 4b-design-and-secure: la nube, 14 cargas de trabajo estándar	opensearch-audit-logging-en abled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearc h de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
sección 4b-design-and-secure: la nube: 15 cargas de trabajo estándar	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
b-design-and-securesección 4: la nube: 15 cargas de trabajo estándar	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
sección 4: la nube, 15 b-design-and-secure cargas de trabajo estándar	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearc h Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 15 cargas de trabajo estándar b-design-and-secure	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
sección 4: la nube, 15 b-design-and-secure cargas de trabajo estándar	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: 15 cargas de trabajo estándar en la nube	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
sección 4: la nube, 15 cargas de trabajo estándar b-design-and-secure	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
sección 4: la nube, 15 cargas de trabajo estándar b-design-and-secure	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
sección 4: la nube, 15 b-design-and-secure cargas de trabajo estándar	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
sección 4:15 cargas de trabajo estándar en la nube b-design-and-secure	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.
sección 4b-design-and-secure: la nube, 15 cargas de trabajo estándar	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
sección 4 -1c-run-the-cloud: cargas de trabajo estándar	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de administración y las llamadas a la API. AWS Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 2: cargas de trabajo estándar	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.
sección 4c-run-the-cloud: 2: cargas de trabajo estándar	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 2: cargas de trabajo estándar	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.
sección 4:2: cargas de trabajo estándar c-run-the-cloud	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 2: cargas de trabajo estándar	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
sección 4:2: cargas de trabajo estándar c-run-the-cloud	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4 -2: cargas c-run-the-cloud de trabajo estándar	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
sección 4:2: cargas de trabajo estándar c-run-the-cloud	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
sección 4:2: cargas de trabajo estándar c-run-the-cloud	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
sección 4c-run-the-cloud: 2: cargas de trabajo estándar	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
sección 4:3: cargas de trabajo estándar c-run-the-cloud	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
sección 4 -3c-run-the-cloud: cargas de trabajo estándar	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de administración y las llamadas a la API. AWS Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	AWS Regla de configuración	Directrices
c-run-the-cloudsección 4:3: cargas de trabajo estándar	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	multi-region-cloudtrail-enabled	AWS CloudTrail registra AWS las acciones de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
c-run-the-cloudsección 4:3: cargas de trabajo estándar	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3c-run-the-cloud: cargas de trabajo estándar	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
sección 4:3: cargas de trabajo estándar c-run-the-cloud	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
sección 4 -3: cargas c-run-the-cloud de trabajo estándar	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
sección 4c-run-the-cloud: 3: cargas de trabajo estándar	opensearch-audit-logging-en abled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearc h de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 4: cargas de trabajo estándar	response-plan-exists-maintained (verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable.
sección 4 -5c-run-the-cloud: cargas de trabajo estándar	autoscaling-group-elb-healthcheck- obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.
sección 4 -5c-run-the-cloud: cargas de trabajo estándar	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 5: cargas de trabajo estándar	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	AWS Regla de configuración	Directrices
sección 4:5: cargas de trabajo estándar c-run-the-cloud	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de actividad que puede soportar cada mesa. read/write DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentag e de cuenta (Config Default: 80). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 5: cargas de trabajo estándar	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
sección 4 -5c-run-the-cloud: cargas de trabajo estándar	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	AWS Regla de configuración	Directrices
sección 4 -5: cargas c-run-the-cloud de trabajo estándar	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	AWS Regla de configuración	Directrices
sección 4 -5: cargas c-run-the-cloud de trabajo estándar	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	AWS Regla de configuración	Directrices
c-run-the-cloudsección 4:6 cargas de trabajo estándar	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
sección 4c-run-the-cloud: 6 cargas de trabajo estándar	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
sección 4c-run-the-cloud: 6 cargas de trabajo estándar	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
sección 4:6 cargas de trabajo estándar c-run-the-cloud	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para cargas de trabajo estándar ABS CCIG 2.0.

Prácticas operativas recomendadas para ACSC Essential 8

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el modelo Essential Eight Maturity del Centro de Ciberseguridad de Australia (ACSC) y las reglas de Config AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles ACSC Essential Eight. Un control ACSC Essential Eight puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones. Algunas de las asignaciones a reglas de Config son para la sección de orden superior

(por ejemplo, estrategias de mitigación para limitar el alcance de los incidentes de ciberseguridad), a diferencia de las secciones más prescriptivas.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones a controles del ACSC Essential 8, creado por la Commonwealth de Australia y que está disponible en ACSC | Essential Eight. La licencia del marco en virtud de la Creative Commons Attribution 4.0 International Public License y la información sobre los derechos de autor del marco (incluida la exención de garantías) se pueden consultar en ACSC | Copyright.

ID de control	AWS Regla de configuración	Directrices
Application_control	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
Application_control	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada

ID de control	AWS Regla de configuración	Directrices
		a una ACL web de WAF para protegerla de ataques maliciosos.
Application_control	cloudwatch-log-group-encrypted	Comprueba si los grupos de CloudWatch registro de Amazon están cifrados con alguna clave de AWS KMS o con un identificador de clave de AWS KMS específico. La regla no cumple con los requisitos si un grupo de CloudWatch registros no se cifra con una clave de KMS o se cifra con una clave de KMS que no se proporciona en el parámetro de la regla.

ID de control	AWS Regla de configuración	Directrices
Application_control	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
Application_control	waf-regional-rule-not-vacío	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencadenar un comportamiento no deseado.
Application_control	waf-regional-rulegroup-not-vacío	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportamiento no deseado.

ID de control	AWS Regla de configuración	Directrices
Application_control	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.
Application_control	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
Patch_applications	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.
Patch_applications	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
Patch_applications	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.
Patch_applications	ec2- -ami instance-launched-with-allowed	Comprueba si las instancias EC2 en ejecución o detenidas se lanzaron con Amazon Machine Images (AMIs) que cumplen AMIs los criterios permitidos. La regla no es compatible si una AMI no cumple con los AMIs criterios permitidos y la AMIs configuración permitida no está deshabilitada.

ID de control	AWS Regla de configuración	Directrices
Patch_applications	elastic-beanstalk-managed-updates-activado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
Patch_applications	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	AWS Regla de configuración	Directrices
Patch_applications	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
Patch_applications	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	iam-no-inline-policy-marcar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
Restrict_administrative_privileges	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
Restrict_administrative_privileges	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabilitada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.
Restrict_administrative_privileges	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).
Restrict_administrative_privileges	efs-access-point-enforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	iam-user-group-membership-compruebe	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Restrict_administrative_privileges	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	rds-instance-iam-authentication-activado	Asegúrese de que la autenticación AWS Identity and Access Management (IAM) esté habilitada en las instancias del Amazon Relational Database Service (Amazon RDS) para controlar el acceso a los sistemas y activos. De esta manera se fuerza el cifrado del tráfico de red hacia y desde la base de datos mediante la capa de sockets seguros (SSL). No es necesario almacenar credenciales de usuario en la base de datos, ya que la autenticación se administra de forma externa.
Restrict_administrative_privileges	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomiend a utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Restrict_administrative_privileges	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Patch_operating_systems	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
Multi-factor_authentication	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
Multi-factor_authentication	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
Multi-factor_authentication	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
Multi-factor_authentication	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
Multi-factor_authentication	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
Regular_backups	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	AWS Regla de configuración	Directrices
Regular_backups	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
Regular_backups	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Regular_backups	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Regular_backups	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	AWS Regla de configuración	Directrices
Regular_backups	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
Regular_backups	s3- bucket-default-lock-enabled	Comprueba si el bucket de S3 tiene habilitado el bloqueo de forma predeterminada. La regla es NON_COMPLIANT si el bloqueo no está habilitado.

ID de control	AWS Regla de configuración	Directrices
Regular_backups	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
Regular_backups	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	AWS Regla de configuración	Directrices
Regular_backups	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Regular_backups	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	AWS Regla de configuración	Directrices
Regular_backups	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.
Regular_backups	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Regular_backups	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el ACSC Essential 8.

Prácticas operativas recomendadas para ACSC ISM: parte 1

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el Manual de seguridad de la información (ISM) 2020-06 del Centro de Ciberseguridad de Australia (ACSC) y las reglas de AWS Config administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de ISM. Un control del ISM puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones a controles dentro del marco del ISM, creado por la Commonwealth de Australia y que está disponible en el Australian Government Information Security Manual. La licencia del marco en virtud de la Creative Commons Attribution 4.0 International Public License y la información sobre los derechos de autor del marco (incluida la exención de garantías) se pueden consultar en ACSC | Copyright.

ID de control	AWS Regla de configuración	Directrices
43	response-plan-exists-maintained (verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable.
252	security-awareness-program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
261	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
261	elb-logging-enabled	La actividad de Elastic Load Balancing (ELB) es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los

ID de control	AWS Regla de configuración	Directrices
		datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
261	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS WAF El registro proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que se AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	AWS Regla de configuración	Directrices
298	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen con AWS Systems Manager lo exigido por las políticas y los procedimientos de su organización.

ID de control	AWS Regla de configuración	Directrices
298	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
298	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
298	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (Amazon RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	AWS Regla de configuración	Directrices
380	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.
459	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
459	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.

ID de control	AWS Regla de configuración	Directrices
459	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
459	efs-encrypted-check	Puesto que puede haber información confidencial, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (Amazon EFS).
459	encrypted-volumes	Puesto que puede haber información confidencial, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
459	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
459	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
459	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service(AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
459	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Regla de configuración	Directrices
459	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
459	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté activado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
459	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service(AWS KMS) esté activado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker bloc de notas, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
459	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS Backup de recuperación. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
459	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado de tus AWS CodeBuild artefactos esté activado.
459	codebuild-project-sCifrado con 3 registros	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para AWS CodeBuild los registros almacenados en Amazon S3.
459	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
459	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.
459	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
459	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitad o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
459	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado mediante AWS Key Management Service ().AWS KMS Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
580	audit-log-policy-exists (verificación del proceso)	Establezca y mantenga una política de administración de registros de auditoría que defina los requisitos de registro de su organización. Esto incluye, pero no se limita a, la revisión y la conservación de los registros de auditoría.
634	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
859	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.
974	iam-user-mfa-enabled	Habilite esta regla para restringir el acceso a los recursos en la Nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
974	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos de la Nube de AWS asegurándose de que la MFA esté habilitada para todos los usuarios AWS Identity and Access Management(IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
1139	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcio nan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográ ficos de alta seguridad. Esta regla requiere que establezc a una política de seguridad predefinida para sus oyentes de SSL. La política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
1173	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
1173	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
1173	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
1173	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
1173	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
1228	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
1240	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
1240	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
1271	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
1271	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuac ión, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	AWS Regla de configuración	Directrices
1277	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
1277	rds-instance-iam-authentication-habilitado	Asegúrese de que la autenticación AWS Identity and Access Management (IAM) esté habilitada en las instancias del Amazon Relational Database Service (Amazon RDS) para controlar el acceso a los sistemas y activos. De esta manera se fuerza el cifrado del tráfico de red hacia y desde la base de datos mediante la capa de sockets seguros (SSL). No es necesario almacenar credenciales de usuario en la base de datos, ya que la autenticación se administra de forma externa.

ID de control	AWS Regla de configuración	Directrices
1277	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
1380	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	AWS Regla de configuración	Directrices
1380	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1380	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.
1380	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
1380	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancia s de Amazon Relational Database Service (RDS) para garantizar que estén instalada s las últimas actualizaciones de las versiones secundari as del sistema de administr ación de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.
1380	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1380	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
1380	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
1380	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
1380	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
1380	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabilitada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.

ID de control	AWS Regla de configuración	Directrices
1380	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.
1380	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	AWS Regla de configuración	Directrices
1380	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).
1380	efs-access-point-enforce-id entidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicació n por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitad o, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	AWS Regla de configuración	Directrices
1380	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
1380	rds-instance-iam-authentication-habilitado	Asegúrese de que la autenticación AWS Identity and Access Management (IAM) esté habilitada en las instancias del Amazon Relational Database Service (Amazon RDS) para controlar el acceso a los sistemas y activos. De esta manera se fuerza el cifrado del tráfico de red hacia y desde la base de datos mediante la capa de sockets seguros (SSL). No es necesario almacenar credenciales de usuario en la base de datos, ya que la autenticación se administra de forma externa.

ID de control	AWS Regla de configuración	Directrices
1380	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
1380	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
1380	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
1380	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomiend a utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
1380	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
1388	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
1388	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
1401	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
1401	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
1401	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
1401	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
1401	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
1402	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
1404	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
1405	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
1405	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
1405	multi-region-cloudtrail-enabled	MULTI_REGION_CLOUD_TRAIL_ENABLED

ID de control	AWS Regla de configuración	Directrices
1405	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
1405	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
1405	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
1405	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
1405	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	AWS Regla de configuración	Directrices
1405	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
1405	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
1405	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
1405	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
1405	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilad os proporcionan información detallada sobre las solicitud es enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
1405	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.
1405	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.
1405	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	AWS Regla de configuración	Directrices
1405	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
1490	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
1490	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
1490	waf-regional-rule-not-vacío	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencade nar un comportamiento no deseado.
1490	waf-regional-rulegroup-not-vacío	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportam iento no deseado.

ID de control	AWS Regla de configuración	Directrices
1490	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.
1490	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1501	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
1504	iam-root-access-key-comprob ar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorpora r el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
1504	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
1504	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
1504	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
1504	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
1509	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
1509	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
1509	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
1509	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
1509	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
1509	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
1509	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
1509	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	AWS Regla de configuración	Directrices
1509	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
1509	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
1509	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
1509	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
1509	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilad os proporcionan información detallada sobre las solicitud es enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
1509	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.
1509	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.
1509	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	AWS Regla de configuración	Directrices
1509	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
1511	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	AWS Regla de configuración	Directrices
1511	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
1511	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	AWS Regla de configuración	Directrices
1511	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
1511	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
1511	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	AWS Regla de configuración	Directrices
1511	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
1511	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.
1511	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatiz adas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantán ea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	AWS Regla de configuración	Directrices
1511	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
1511	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	AWS Regla de configuración	Directrices
1511	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	AWS Regla de configuración	Directrices
1511	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
1511	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalment e administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
1511	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
1511	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	AWS Regla de configuración	Directrices
1511	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.
1515	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	AWS Regla de configuración	Directrices
1515	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
1515	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
1515	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
1515	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	AWS Regla de configuración	Directrices
1515	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
1515	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
1515	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.
1515	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
1515	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	AWS Regla de configuración	Directrices
1515	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.
1515	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
1515	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
1536	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
1537	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
1537	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
1552	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.
1552	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
1552	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
1552	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
1552	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
1579	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
1580	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	AWS Regla de configuración	Directrices
1580	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
1580	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
1650	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
1650	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
1650	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
1650	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
1650	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
1650	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
1650	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
1650	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	AWS Regla de configuración	Directrices
1650	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
1650	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
1650	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
1650	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
1650	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilad os proporcionan información detallada sobre las solicitud es enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
1650	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.
1650	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.
1650	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	AWS Regla de configuración	Directrices
1650	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
1657	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
1657	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
1657	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1657	waf-regional-rule-not-vacío	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencadenar un comportamiento no deseado.
1657	waf-regional-rulegroup-not-vacío	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportamiento no deseado.
1657	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.

ID de control	AWS Regla de configuración	Directrices
1657	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.
1661	cloud-trail-cloud-watch-hab ilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
1661	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
1661	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
1661	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
1661	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
1661	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
1661	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
1661	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	AWS Regla de configuración	Directrices
1661	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
1661	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
1661	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
1661	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
1661	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilad os proporcionan información detallada sobre las solicitud es enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
1661	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
1679	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
1679	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
1679	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
1679	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
1679	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
1680	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
1680	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
1680	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
1680	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
1680	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
1681	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
1681	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
1681	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
1681	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
1681	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
1683	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
1683	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
1690	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.
1690	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1690	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.
1690	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
1690	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancia s de Amazon Relational Database Service (RDS) para garantizar que estén instalada s las últimas actualizaciones de las versiones secundari as del sistema de administr ación de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.
1690	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1690	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
1691	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.
1691	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1691	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.
1691	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
1691	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancia s de Amazon Relational Database Service (RDS) para garantizar que estén instalada s las últimas actualizaciones de las versiones secundari as del sistema de administr ación de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.
1691	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1691	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
1693	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.
1693	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1693	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.
1693	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
1693	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancia s de Amazon Relational Database Service (RDS) para garantizar que estén instalada s las últimas actualizaciones de las versiones secundari as del sistema de administr ación de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.
1693	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
1693	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
1694	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
1695	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
1707	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.
P1	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
P1	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
P3	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	AWS Regla de configuración	Directrices
P5	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
P7	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
P7	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
P7	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
P7	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	AWS Regla de configuración	Directrices
P8	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
P9	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
P9	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	AWS Regla de configuración	Directrices
P9	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
P9	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	AWS Regla de configuración	Directrices
P9	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	AWS Regla de configuración	Directrices
P9	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.
P9	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
P9	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
P9	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
P9	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
P9	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	AWS Regla de configuración	Directrices
P9	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalment e administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
P9	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
P9	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
P10	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
P10	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
P10	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
P10	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomiend a utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
P10	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
P11	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

Plantilla

Estas plantillas están disponibles en: GitHub

- Prácticas operativas recomendadas para ACSC ISM: parte 1
- Prácticas operativas recomendadas para ACSC ISM: parte 2

Prácticas operativas recomendadas para ACSC ISM: parte 2

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporcionan ejemplos adicionales de mapeo entre el Manual de seguridad de la información (ISM) 2020-06 del Centro de Ciberseguridad de Australia (ACSC) y las reglas de AWS Config administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de ISM. Un control del ISM puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones a controles dentro del marco del ISM, creado por la Commonwealth de Australia y que está disponible en el Australian Government Information Security Manual. La licencia del marco en virtud de la Creative Commons Attribution 4.0 International Public License y la información sobre los derechos de autor del marco (incluida la exención de garantías) se pueden consultar en ACSC | Copyright.

ID de control	AWS Regla de configuración	Directrices
1984	appmesh-virtual-gateway-backend-defaults-tls	Comprueba si los valores predeterminados del backend para las puertas de enlace virtuales requieren que las puertas de enlace AWS App Mesh virtuales se comunique n con todos los puertos mediante TLS. La regla no cumple con los requisito s de Configuration.spec. BackendDefaults. ClientPol icy.Tls.Enforce es falso.

ID de control	AWS Regla de configuración	Directrices
1984	appmesh-virtual-node-backend-defaults-tls-on	Comprueba si los valores predeterminados del backend para los nodos AWS App Mesh virtuales requieren que los nodos virtuales se comuniquen con todos los puertos mediante TLS. La regla no cumple con los requisitos de Configuration.spec. BackendDefaults. ClientPolicy.Tls.Enforce es falso.
1984	msk-in-cluster-node-require-tls	Comprueba si un clúster de Amazon MSK está cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.

ID de control	AWS Regla de configuración	Directrices
1984	rds-mysql-instance-encrypted-en tránsito	Comprueba si las conexiones a las instancias de bases de datos de Amazon RDS para MySQL están configuradas para utilizar el cifrado en tránsito. La regla es NON_COMPLIANT si el grupo de parámetros de base de datos asociado no está sincronizado o si el parámetro require_secure_transport no está establecido en 1.
1984	rds-postgres-instance-encrypted-en tránsito	Comprueba si las conexiones a instancias de bases de datos de Amazon RDS para PostgreSQL están configuradas para utilizar cifrado en tránsito. La regla es NON_COMPLIANT si el grupo de parámetros de base de datos asociado no está sincronizado o si el parámetro rds.force_ssl no está establecido en 1.

ID de control	AWS Regla de configuración	Directrices
1985	ebs-snapshot-public-restorable-comprobar	Comprueba si las instantáneas de Amazon Elastic Block Store (Amazon EBS) no se pueden restaurar públicamente. La regla es NON_COMPLIANT si una o más instantáneas con el RestorableByUserIds campo están configuradas como todas, es decir, las instantáneas de Amazon EBS son públicas.
1985	s3- bucket-mfa-delete-enabled	Comprueba si las instantáneas de Amazon Elastic Block Store (Amazon EBS) no se pueden restaurar públicamente. La regla es NON_COMPLIANT si una o más instantáneas con el RestorableByUserIds campo están configuradas como todas, es decir, las instantáneas de Amazon EBS son públicas.

ID de control	AWS Regla de configuración	Directrices
1985	s3- bucket-public-read-prohibited	Comprueba si sus buckets de Amazon S3 no permiten acceso de lectura público. La regla comprueba la configuración de Block Public Access, la política del bucket y la lista de control de acceso (ACL) del bucket. La regla se cumple cuando se dan las dos condiciones siguientes: • La configuración de Block Public Access restringe las políticas públicas o la política del bucket no permite el acceso de lectura público. • La configuración Bloquear el acceso público restringe el acceso público ACLs o la ACL del bucket no permite el acceso de lectura público. La regla no se cumple en los siguientes casos: • Si la configuración Bloquear el acceso público no restringe las políticas públicas, AWS Config evalúa si la política permite el acceso de lectura público. Si la política permite acceso

ID de control	AWS Regla de configuración	Directrices
		de lectura público, la regla no se cumple. • Si la configuración Bloquear el acceso público no restringe el depósito público ACLs, AWS Config evalúa si la ACL del depósito permite el acceso de lectura público. Si la ACL del bucket permite acceso de lectura público, la regla no se cumple.

ID de control	AWS Regla de configuración	Directrices
1985	s3- bucket-public-write-prohibited	Comprueba si sus buckets de Amazon S3 no permiten acceso de escritura público. La regla comprueba la configuración de Block Public Access, la política del bucket y la lista de control de acceso (ACL) del bucket. La regla se cumple cuando se dan las dos condiciones siguientes: • La configuración de Block Public Access restringe las políticas públicas o la política del bucket no permite el acceso de escritura público. • La configuración Bloquear el acceso público restringe el acceso público ACLs o la ACL del bucket no permite el acceso de escritura público. La regla no se cumple en los siguientes casos: • Si la configuración Bloquear el acceso público no restringe las políticas públicas, AWS Config evalúa si la política permite el acceso de escritura

ID de control	AWS Regla de configuración	Directrices
		público. Si la política permite el acceso de escritura público, la regla no se cumple. • Si la configuración Bloquear el acceso público no restringe el segmento público ACLs, AWS Config evalúa si la ACL del segmento permite el acceso de escritura público. Si la ACL del bucket permite el acceso de escritura público, la regla no se cumple.
1985	aurora-resources-in-logically-air-gapped-vault	Comprueba si los clústeres de bases de datos de Amazon Aurora están en un almacén aislado lógicamente. La regla es NON_COMPLIANT si hay un clúster de base de datos de Amazon Aurora que no está en un almacén aislado lógicamente dentro del período de tiempo especific ado.

ID de control	AWS Regla de configuración	Directrices
1985	ebs-resources-in-logically-air-gapped-vault	Comprueba si los volúmenes de Amazon Elastic Block Store (Amazon EBS) están dentro de un almacén aislado lógicamente. La regla es NON_COMPLIANT si hay un volumen de Amazon EBS que no está en un almacén aislado lógicamente dentro del período de tiempo especific ado.
1985	ec2- -gapped-vault resources-in-logically-air	Comprueba si las instancia s de Amazon Elastic Block Store (Amazon EBS) están dentro de un almacén aislado lógicamente. La regla es NON_COMPLIANT si hay una instancia de Amazon EBS que no está en un almacén aislado lógicamente dentro del período de tiempo especific ado.
1985	efs-resources-in-logically-air-gapped-vault	Comprueba si los sistemas de archivos de Amazon Elastic File System (Amazon EFS) están dentro de un almacén aislado lógicamente. La regla es NON_COMPLIANT si hay una sistema de archivos de Amazon EFS que no está en un almacén aislado lógicamen te dentro del período de tiempo especificado.

ID de control	AWS Regla de configuración	Directrices
1985	s3- resources-in-logically-air - bóveda con huecos	Comprueba si los buckets de Amazon Simple Storage Service (Amazon S3) están dentro de un almacén aislado lógicamente. La regla es NON_COMPLIANT si hay un bucket de Amazon S3 que no está en un almacén aislado lógicamente dentro del período de tiempo especific ado.

Plantilla

Esta plantilla está disponible en GitHub: Mejores prácticas operativas para el ACSC ISM, parte 2.

Prácticas operativas recomendadas para IA y ML

Este paquete de conformidad contiene AWS Config reglas basadas en IA y ML. Para ver una lista de todas las reglas administradas compatibles AWS Config, consulta la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para IA y aprendizaje automático.

Prácticas operativas recomendadas para Amazon API Gateway

Este paquete de conformidad contiene AWS Config reglas basadas en el uso de Amazon API Gateway en su interior AWS. Para ver una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Operational Best Practices for Amazon API Gateway.

Mejores prácticas operativas para Amazon CloudWatch

Este paquete de conformidad contiene AWS Config reglas basadas en el uso de Amazon CloudWatch en AWSél. Para ver una lista de todas las reglas gestionadas compatibles AWS Config, consulta la Lista de reglas AWS Config gestionadas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Operational Best Practices for Amazon CloudWatch.

Prácticas operativas recomendadas para Amazon DynamoDB

La plantilla está disponible en GitHub: Operational Best Practices for Amazon DynamoDB.

Prácticas operativas recomendadas para Amazon S3

La plantilla está disponible en GitHub: Operational Best Practices for Amazon S3.

Prácticas operativas recomendadas para APRA CPG 234

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre la CPG 234 de la Autoridad de Regulación Prudencial de Australia (APRA) y las reglas de AWS Config administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles APRA CPG 234. Un control de APRA CPG 234 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones a controles dentro del marco de APRA CPG 234 2019, creado por la Commonwealth de Australia y que está disponible en Prudential Practice Guide: CPG 234 Information Security. La licencia del marco en virtud de la Creative Commons Australia Attribution 3.0 Licence y la información sobre los derechos de autor del marco (incluida la exención de garantías) se pueden consultar en APRA | Copyright.

ID de control	AWS Regla de configuración	Directrices
36a	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
36a	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
36a	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
36b	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
36b	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.
36b	ec2- -comprobar managedin stance-patch-compliance-sta tus	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
36b	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	AWS Regla de configuración	Directrices
36b	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
36b	elastic-beanstalk-managed-updates-activado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
36b	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	AWS Regla de configuración	Directrices
36c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
36c	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
36c	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
36c	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
36c	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
36c	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
36c	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
36c	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegi os de los necesarios para completar una tarea puede infringir el principio de privilegi o mínimo y la separación de funciones.
36c	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
36d	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
36d	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
36d	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36d	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
36d	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36d	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
36d	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
36d	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
36d	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
36d	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
36d	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36d	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
36d	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
36d	s3- bucket-public-write-prohibi ted	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
36d	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
36d	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
36d	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
36d	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
36d	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
36d	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
36d	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
36d	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
36d	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
36d	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
36d	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
36d	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
36d	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
36d	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	AWS Regla de configuración	Directrices
36d	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
36d	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
36d	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.
36d	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	AWS Regla de configuración	Directrices
36d	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
36d	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.
36d	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
36d	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
36d	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
36d	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
36d	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	AWS Regla de configuración	Directrices
36d	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
36d	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	AWS Regla de configuración	Directrices
36d	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
36e	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	AWS Regla de configuración	Directrices
36e	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
36e	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
36e	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36e	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
36e	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearc h Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
36e	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36e	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
36e	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
36e	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
36e	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
36e	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
36e	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36e	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
36e	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
36e	s3- bucket-public-write-prohibi ted	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
36e	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
36e	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
36e	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
36e	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
36e	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
36e	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
36e	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	AWS Regla de configuración	Directrices
36e	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
36e	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
36e	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	AWS Regla de configuración	Directrices
36e	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
36f	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36f	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
36f	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36f	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
36f	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36f	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
36f	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
36f	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
36f	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
36f	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
36f	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
36f	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
36f	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
36f	s3- bucket-public-write-prohibi ted	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
36f	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
36f	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
36f	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.
36f	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
36f	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
36f	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
36f	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
36f	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
36f	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
36f	autoscaling-launch-config-p ublic-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidore s.

ID de control	AWS Regla de configuración	Directrices
36f	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.
36f	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
36f	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
36f	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	AWS Regla de configuración	Directrices
36f	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
36g	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
36g	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
36g	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
36h	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
36h	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
36h	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
36h	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
36h	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
36h	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
36h	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
36h	elastic-beanstalk-managed-updates-activado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
36i	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	AWS Regla de configuración	Directrices
36i	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Regla de configuración	Directrices
36i	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentag e de cuenta (Config Default: 80). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
36i	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
36i	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.
36i	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	AWS Regla de configuración	Directrices
36i	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	AWS Regla de configuración	Directrices
36i	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
36i	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
36i	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.
36i	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
36j	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
36j	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
36j	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.
36j	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
36j	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	AWS Regla de configuración	Directrices
36j	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Regla de configuración	Directrices
36j	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default: 80). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
36j	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notificat ion Service (Amazon SNS) cuando una función falle.
36j	rds-enhanced-monitoring-ena bled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenam iento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implement ación Multi-AZ, se recopilan los datos de cada dispositi vo del host secundario y las métricas del host secundario.

ID de control	AWS Regla de configuración	Directrices
36j	beanstalk-enhanced-health-reporting-activado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.
36j	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
36l	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.
36l	dynamodb-autoscaling-enable d	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimien to aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/writ e capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	AWS Regla de configuración	Directrices
36l	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.
36l	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	AWS Regla de configuración	Directrices
36l	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
36l	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
36l	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
36l	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
36l	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
36l	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
36l	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
36l	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
36l	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	AWS Regla de configuración	Directrices
36l	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
36l	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
36l	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
36l	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	AWS Regla de configuración	Directrices
39(a)(b)(d)	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
39(a)(b)(d)	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
39(a)(b)(d)	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
40	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
40	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
40	elastic-beanstalk-managed-updates-activado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
40	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	AWS Regla de configuración	Directrices
44a	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
44a	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
44a	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
44b	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
44b	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.
44b	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
44c	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
44c	iam-root-access-key-comprob ar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorpora r el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
44c	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
44c	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
45	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
45	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
45	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
45	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
45	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
45	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
45	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
45	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
45	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
45	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
45	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
45	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
45	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
45	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
45	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
45	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
45	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
45	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
45	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
45	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
45	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
45	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
45	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
45	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
45	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
45	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
45	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
45	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
45	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
45	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
45	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
45	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
45	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.
45	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	AWS Regla de configuración	Directrices
45	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegi os de los necesarios para completar una tarea puede infringir el principio de privilegi o mínimo y la separación de funciones.
45	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
45	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
45	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
45	autoscaling-launch-config-p ublic-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidore s.

ID de control	AWS Regla de configuración	Directrices
45	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.
45	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
45	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
45	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	AWS Regla de configuración	Directrices
47c	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
47c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
47c	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
47c	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
47c	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
47c	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
47c	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
52c	api-gw-cache-enabled-y cifrada	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
52c	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
52c	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
52c	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
52c	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
52c	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
52c	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
52c	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
52c	Habilitado para s3 bucket-se rver-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
52c	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
52c	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
52c	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
52c	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
52c	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
52c	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
52c	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
52c	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
52c	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
52d	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
52d	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
52d	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
52d	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
52d	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
52d	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
52d	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
52d	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
52d	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
52d	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
52d	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
52d	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
52d	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
52d	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
52d	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
52d	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
52d	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
52d	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
52d	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	AWS Regla de configuración	Directrices
52d	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
52d	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
52d	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
52d	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
52e	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
52e	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
53	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
53	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
53	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
53	sagemaker-notebook-no-direct-acceso a Internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
53	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
53	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
53	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
53	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
53	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
53	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
53	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
53	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
53	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
53	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
53	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
53	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
53	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
53	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
53	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
53	autoscaling-launch-config-p ublic-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidore s.

ID de control	AWS Regla de configuración	Directrices
53	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	AWS Regla de configuración	Directrices
53	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
53	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	AWS Regla de configuración	Directrices
54	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
54	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExp iration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
54	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
54	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
54	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
54	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
54	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
54	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
54	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
54	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
54	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
54	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
54	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
54	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
54	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
54	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
54	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
54	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
54	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
54	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
54	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
54	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
54	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
54	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
54	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	AWS Regla de configuración	Directrices
54	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
55	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
55	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
67	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
67	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
67	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
67	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
67	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
67	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
67	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
67	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
67	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
67	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	AWS Regla de configuración	Directrices
67	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.
67	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
67	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
67	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
67	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
67	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
67	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
67	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
68	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
68	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
73	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
73	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(b)(h)	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(b)(h)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AttachmentA_1(b)(h)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(b)(h)	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AttachmentA_1(b)(h)	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(b)(h)	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integrada s. Las políticas administr adas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(b)(h)	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(b)(h)	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(b)(h)	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegi os de los necesarios para completar una tarea puede infringir el principio de privilegi o mínimo y la separación de funciones.
AttachmentA_1(b)(h)	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
AttachmentA_1(c)	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(c)	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
AttachmentA_1(e)	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(e)	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
AttachmentA_1(e)	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(e)	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AttachmentA_1(e)	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
AttachmentA_1(e)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(e)	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
AttachmentA_1(e)	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(e)	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(e)	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
AttachmentA_1(e)	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(e)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
AttachmentA_1(e)	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	AWS Regla de configuración	Directrices
AttachmentA_1(e)	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
AttachmentA_1(e)	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
AttachmentB_1	security-awareness-program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
AttachmentC_4	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
AttachmentC_4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegi o y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
AttachmentC_4	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
AttachmentC_4	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
AttachmentC_4	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
AttachmentC_4	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
AttachmentC_4	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.
AttachmentC_4	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_4	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AttachmentC_5	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_5	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
AttachmentC_5	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
AttachmentC_5	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_5	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
AttachmentC_6	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
AttachmentC_6	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
AttachmentC_6	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(c)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
AttachmentC_7(h)	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AttachmentC_7(h)	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(h)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
AttachmentC_7(h)	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(h)	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(h)	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
AttachmentC_7(h)	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(h)	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(h)	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(h)	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
AttachmentC_7(h)	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(h)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
AttachmentC_7(h)	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(h)	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
AttachmentC_7(h)	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(i)	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(j)	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
AttachmentC_7(j)	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_7(j)	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
AttachmentC_7(j)	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
AttachmentC_8	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
AttachmentC_8	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AttachmentC_8	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_8	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
AttachmentC_8	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_8	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_8	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_8	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
AttachmentC_8	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_8	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
AttachmentC_8	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	AWS Regla de configuración	Directrices
AttachmentC_8	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
AttachmentD_1	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	AWS Regla de configuración	Directrices
AttachmentD_1	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personale s ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personale s o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
AttachmentE_4	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
AttachmentE_4	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	AWS Regla de configuración	Directrices
AttachmentE_5(d)	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
AttachmentE_1(a)(b)(d)	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
AttachmentE_1(a)(b)(d)	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
AttachmentE_1(a)(b)(d)	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.
AttachmentE_1(a)(b)(d)	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AttachmentE_1(a)(b)(d)	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
AttachmentE_1(a)(b)(d)	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
AttachmentE_1(a)(b)(d)	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
AttachmentE_1(a)(b)(d)	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
AttachmentE_1(a)(b)(d)	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Regla de configuración	Directrices
AttachmentE_1(a)(b)(d)	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
AttachmentE_1(a)(b)(d)	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
AttachmentE_1(a)(b)(d)	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	AWS Regla de configuración	Directrices
AttachmentE_1(a)(b)(d)	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
AttachmentE_1(a)(b)(d)	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
AttachmentE_1(a)(b)(d)	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
AttachmentE_1(a)(b)(d)	Habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
AttachmentE_1(a)(b)(d)	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AttachmentE_1(a)(b)(d)	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
AttachmentE_1(a)(b)(d)	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
AttachmentE_1(a)(b)(d)	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
AttachmentE_1(a)(b)(d)	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
AttachmentE_1(a)(b)(d)	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
AttachmentE_1(a)(b)(d)	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
AttachmentE_1(a)(b)(d)	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AttachmentE_1(a)(b)(d)	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
AttachmentE_1(a)(b)(d)	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el APRA CPG 234.

Prácticas operativas recomendadas para la gestión de activos

Este paquete de conformidad contiene AWS Config reglas basadas en la gestión de activos interna AWS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para la gestión de activos.

Mejores prácticas operativas para AWS Backup

Este paquete de conformidad contiene AWS Config reglas basadas AWS Backup en AWS ellas. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para AWS Backup.

Prácticas operativas recomendadas para AWS Identity and Access Management

La plantilla está disponible en GitHub: Operational Best Practices for AWS Identity and Access Management.

Mejores prácticas operativas para el pilar de confiabilidad de AWS un marco de trabajo bien diseñado

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el pilar de confiabilidad del marco de trabajo de Well-Architected de Amazon Web Services y AWS las reglas de Config administradas.

Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más de los principios de diseño del pilar. Una categoría de Well-Architected Framework puede estar relacionada con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-1	¿Cómo administra las cuotas de servicio y las restricciones? Para las arquitecturas de carga de trabajo basadas en la nube, existen cuotas de servicio (que también se denominan límites de servicio). Estas cuotas existen para evitar el aprovisio namiento accidental de más recursos de los que se necesitan y para limitar las tasas de solicitud es en las operacion es de la API a fin de proteger los servicios contra el abuso. También hay limitacio nes de recursos, por ejemplo, la velocidad a la que se pueden introducir bits por un cable de fibra óptica o la cantidad	dynamodb-throughpu t-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/ write actividad que puede soportar cada mesa. DynamoDB utiliza esta informaci ón para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalm ente los parámetro s de RCUThreshold porcentaje de cuenta

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de almacenamiento en un disco físico.		(Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default: 80). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-1	¿Cómo administra las cuotas de servicio y las restricciones? Para las arquitecturas de carga de trabajo basadas en la nube, existen cuotas de servicio (que también se denominan límites de servicio). Estas cuotas existen para evitar el aprovisio namiento accidental de más recursos de los que se necesitan y para limitar las tasas de solicitud es en las operacion es de la API a fin de proteger los servicios contra el abuso. También hay limitacio nes de recursos, por ejemplo, la velocidad a la que se pueden introducir bits por un cable de fibra óptica o la cantidad de almacenamiento en un disco físico.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultane idad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-1	¿Cómo administra las cuotas de servicio y las restricciones? Para las arquitecturas de carga de trabajo basadas en la nube, existen cuotas de servicio (que también se denominan límites de servicio). Estas cuotas existen para evitar el aprovisio namiento accidental de más recursos de los que se necesitan y para limitar las tasas de solicitud es en las operacion es de la API a fin de proteger los servicios contra el abuso. También hay limitacio nes de recursos, por ejemplo, la velocidad a la que se pueden introducir bits por un cable de fibra óptica o la cantidad de almacenamiento en un disco físico.	ecs-task-definition-memory-límite estricto	Limitar el máximo de memoria disponible para los contenedo res de Amazon Elastic Container Service (ECS) garantiza que no se haga un uso indebido de los recursos en caso de que se produzca un acceso malintencionado a los contenedores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-2	¿Cómo planifica la topología de la red? Las cargas de trabajo suelen existir en varios entornos. Estos incluyen varios entornos de nube (tanto de acceso público como privados) y, posiblemente, la infraestructura de su centro de datos existente. Los planes deben incluir consideraciones sobre la red, como la conectividad dentro y entre sistemas, la administración de direcciones IP públicas, la administración de direcciones IP privadas y la resolución de nombres de dominio.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-2	¿Cómo planifica la topología de la red? Las cargas de trabajo suelen existir en varios entornos. Estos incluyen varios entornos de nube (tanto de acceso público como privados) y, posiblemente, la infraestructura de su centro de datos existente. Los planes deben incluir consideraciones sobre la red, como la conectividad dentro y entre sistemas, la administración de direcciones IP públicas, la administración de direcciones IP privadas y la resolución de nombres de dominio.	redshift-enhanced-vpc-routing-habilitada	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-2	¿Cómo planifica la topología de la red? Las cargas de trabajo suelen existir en varios entornos. Estos incluyen varios entornos de nube (tanto de acceso público como privados) y, posiblemente, la infraestructura de su centro de datos existente. Los planes deben incluir consideraciones sobre la red, como la conectividad dentro y entre sistemas, la administración de direcciones IP públicas, la administración de direcciones IP privadas y la resolución de nombres de dominio.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
REL-5	¿Cómo se diseñan las interacciones en un sistema distribuido para mitigar o resistir los errores? Los sistemas distribuidos se basan en las redes de comunicaciones para interconectar componentes, como servidores o servicios . Su carga de trabajo debe funcionar de manera fiable a pesar de la pérdida de datos o la latencia en estas redes. Los component es del sistema distribuido deben funcionar de manera que no afecten negativamente a otros component es o a la carga de trabajo. Estas prácticas recomenda das previenen los fallos y mejoran el tiempo medio entre errores (MTBD).	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	api-gw-xray-enabled	AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Asegúrese de que X-Ray esté habilitado para que pueda ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a AWS los recursos descendentes, los microservicios, las bases de datos y la web HTTP. APIs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	ecs-container-insights-enabled	La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon Elastic Container Service (ECS) y sus AWS soluciones. Información de contenedores también proporciona información de diagnóstico, como, por ejemplo, errores de reinicio de contenedores, para ayudarlo a aislar problemas y solucionarlos rápidamente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-6	¿Cómo se supervisan los recursos de la carga de trabajo? Los registros y las métricas son herramientas poderosas para obtener información sobre el estado de su carga de trabajo. Puede configurar su carga de trabajo para supervisar los registros y las métricas y enviar notificaciones cuando se superen los umbrales o se produzcan eventos significativos. La supervisión le permite a su carga de trabajo reconocer cuándo se superan los umbrales de bajo rendimiento o si se producen errores, de modo que pueda recuperarse automáticamente en respuesta a ellos.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-7	¿Cómo diseña su carga de trabajo para adaptarla a los cambios de la demanda? Una carga de trabajo escalable proporciona elasticidad para agregar o eliminar recursos automáticamente, de modo que se ajusten perfectamente a la demanda actual en cualquier momento dado.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-7	¿Cómo diseña su carga de trabajo para adaptarla a los cambios de la demanda? Una carga de trabajo escalable proporciona elasticidad para agregar o eliminar recursos automáticamente, de modo que se ajusten perfectamente a la demanda actual en cualquier momento dado.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-7	¿Cómo diseña su carga de trabajo para adaptarla a los cambios de la demanda? Una carga de trabajo escalable proporciona elasticidad para agregar o eliminar recursos automáticamente, de modo que se ajusten perfectamente a la demanda actual en cualquier momento dado.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-8	¿Cómo implement a el cambio? Los cambios controlados son necesarios para implementar nuevas funcionalidades y garantizar que las cargas de trabajo y el entorno operativo ejecuten software conocido y se puedan parchear o reemplaza r de forma predecible. Si estos cambios no se controlan, es difícil predecir su efecto o abordar los problemas que surjan a causa de ellos.	redshift-cluster-m aintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configura ción preferida para su organización. En concreto, que tengan períodos de mantenimi ento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que establezc as el. allowVers ionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
REL-8	¿Cómo implement a el cambio? Los cambios controlados son necesarios para implementar nuevas funcionalidades y garantizar que las cargas de trabajo y el entorno operativo ejecuten software conocido y se puedan parchear o reemplaza r de forma predecible. Si estos cambios no se controlan, es difícil predecir su efecto o abordar los problemas que surjan a causa de ellos.	rds-automatic-mino r-version-habilitada para la actualización	Habilite las actualiza ciones automátic as de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundari as del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correccio nes de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-8	¿Cómo implement a el cambio? Los cambios controlados son necesarios para implementar nuevas funcionalidades y garantizar que las cargas de trabajo y el entorno operativo ejecuten software conocido y se puedan parchear o reemplaza r de forma predecible. Si estos cambios no se controlan, es difícil predecir su efecto o abordar los problemas que surjan a causa de ellos.	ec2- -check managedinstance-pa tch-compliance-status	Habilite esta regla para ayudar a identific ar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimi entos de su organizac ión en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-8	¿Cómo implement a el cambio? Los cambios controlados son necesarios para implementar nuevas funcionalidades y garantizar que las cargas de trabajo y el entorno operativo ejecuten software conocido y se puedan parchear o reemplaza r de forma predecible. Si estos cambios no se controlan, es difícil predecir su efecto o abordar los problemas que surjan a causa de ellos.	ec2- -check managedinstance-as sociation-compliance-status	Use AWS Systems Manager Associati ons para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancia s administradas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con sus requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-9	¿Cómo se hace una copia de seguridad de los datos? Realice copias de seguridad de los datos, las aplicaciones y la configuración para cumplir con los requisitos de objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO).	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-10	¿Cómo utiliza el aislamiento de errores para proteger su carga de trabajo? Los límites de errores aislados limitan el efecto de un error dentro de una carga de trabajo a un número limitado de componentes. Los componentes que se encuentran fuera del límite no se ven afectados por el error. Al usar múltiples límites aislados de errores, puede limitar el impacto en su carga de trabajo.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-10	¿Cómo utiliza el aislamiento de errores para proteger su carga de trabajo? Los límites de errores aislados limitan el efecto de un error dentro de una carga de trabajo a un número limitado de componentes. Los componentes que se encuentran fuera del límite no se ven afectados por el error. Al usar múltiples límites aislados de errores, puede limitar el impacto en su carga de trabajo.	clb-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantiza r una alta disponibi lidad, asegúrese de que su ELB tenga instancias registrad as de varias zonas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-10	¿Cómo utiliza el aislamiento de errores para proteger su carga de trabajo? Los límites de errores aislados limitan el efecto de un error dentro de una carga de trabajo a un número limitado de componentes. Los componentes que se encuentran fuera del límite no se ven afectados por el error. Al usar múltiples límites aislados de errores, puede limitar el impacto en su carga de trabajo.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantiza r una alta disponibi lidad, asegúrese de que su ELB tenga instancias registrad as de varias zonas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-10	¿Cómo utiliza el aislamiento de errores para proteger su carga de trabajo? Los límites de errores aislados limitan el efecto de un error dentro de una carga de trabajo a un número limitado de componentes. Los componentes que se encuentran fuera del límite no se ven afectados por el error. Al usar múltiples límites aislados de errores, puede limitar el impacto en su carga de trabajo.	lambda-vpc-multi-az-comprobar	Si su función AWS Lambda está configurada para conectarse a una nube privada virtual (VPC) de su cuenta, implemente la función AWS Lambda en al menos dos zonas de disponibilidad diferentes para asegurarse de que su función esté disponibl e para procesar eventos en caso de una interrupción del servicio en una sola zona.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-10	¿Cómo utiliza el aislamiento de errores para proteger su carga de trabajo? Los límites de errores aislados limitan el efecto de un error dentro de una carga de trabajo a un número limitado de componentes. Los componentes que se encuentran fuera del límite no se ven afectados por el error. Al usar múltiples límites aislados de errores, puede limitar el impacto en su carga de trabajo.	opensearch-data-node-fault-tolerancia	Amazon OpenSearch Service (OpenSearch Servicio) requiere al menos tres nodos de datos para una alta disponibilidad y tolerancia a errores. La implementación de un dominio OpenSearch de servicio con al menos tres nodos de datos garantiza las operaciones del clúster en caso de que un nodo falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-10	¿Cómo utiliza el aislamiento de errores para proteger su carga de trabajo? Los límites de errores aislados limitan el efecto de un error dentro de una carga de trabajo a un número limitado de componentes. Los componentes que se encuentran fuera del límite no se ven afectados por el error. Al usar múltiples límites aislados de errores, puede limitar el impacto en su carga de trabajo.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-10	¿Cómo utiliza el aislamiento de errores para proteger su carga de trabajo? Los límites de errores aislados limitan el efecto de un error dentro de una carga de trabajo a un número limitado de componentes. Los componentes que se encuentran fuera del límite no se ven afectados por el error. Al usar múltiples límites aislados de errores, puede limitar el impacto en su carga de trabajo.	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
REL-10	¿Cómo utiliza el aislamiento de errores para proteger su carga de trabajo? Los límites de errores aislados limitan el efecto de un error dentro de una carga de trabajo a un número limitado de componentes. Los componentes que se encuentran fuera del límite no se ven afectados por el error. Al usar múltiples límites aislados de errores, puede limitar el impacto en su carga de trabajo.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

Plantilla

La plantilla está disponible en GitHub: Operational Best Practices for AWS Well-Architected Reliability Pillar.

Mejores prácticas operativas para el pilar de seguridad de AWS Well-Architected Framework

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el pilar de seguridad del marco de arquitectura Well-Architected de Amazon Web Services y AWS las reglas de Config gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más de los principios de diseño del pilar. Una categoría de Well-Architected Framework puede estar relacionada con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de seguridad. Tome los requisitos y procesos	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que ha definido en materia de excelencia operativa en los niveles organizativo y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse al día con las recomendaciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación le permite escalar sus operaciones de seguridad.		configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelencia operativa en los niveles organizativo y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse al día con las recomendaciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación le permite escalar	mfa-enabled-for-iam-acceso desde la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sus operaciones de seguridad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomenda das generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelenci a operativa en los niveles organizat ivo y de carga de trabajo, y aplíquelo s a todas las áreas. Mantenerse al día con las recomenda ciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatiz ación de los procesos de seguridad, las pruebas y la validació n le permite escalar	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sus operaciones de seguridad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomenda das generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelenci a operativa en los niveles organizat ivo y de carga de trabajo, y aplíquelo s a todas las áreas. Mantenerse al día con las recomenda ciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatiz ación de los procesos de seguridad, las pruebas y la validació n le permite escalar	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sus operaciones de seguridad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelencia operativa en los niveles organizativo y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse al día con las recomendaciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación le permite escalar	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sus operaciones de seguridad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelencia operativa en los niveles organizativo y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse al día con las recomendaciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación le permite escalar	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sus operaciones de seguridad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelencia operativa en los niveles organizativo y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse al día con las recomendaciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación le permite escalar	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sus operaciones de seguridad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelencia operativa en los niveles organizativo y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse al día con las recomendaciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación le permite escalar	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sus operaciones de seguridad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelencia operativa en los niveles organizativo y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse al día con las recomendaciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación le permite escalar	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sus operaciones de seguridad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-1	¿Cómo gestiona su carga de trabajo de forma segura? Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelencia operativa en los niveles organizativo y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse al día con las recomendaciones del sector AWS y la inteligencia sobre amenazas le ayuda a desarrollar su modelo de amenazas y sus objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación le permite escalar	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sus operaciones de seguridad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de operar cargas de AWS trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de operar AWS cargas de trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándo ose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidades que debe gestionar a la hora de operar cargas de AWS trabajo seguras. Comprender el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantizar que las identidades correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidades humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicaciones. Se trata de miembros de su organización o usuarios externos	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidades que debe gestionar a la hora de operar cargas de AWS trabajo seguras. Comprender el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de operar AWS cargas de trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de operar cargas de trabajo seguras AWS . Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidades que debe administrar al abordar la operación de AWS cargas de trabajo seguras. Comprender el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantizar que las identidades correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidades humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicaciones. Se trata de miembros de su organización o usuarios externos	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de gestionar cargas de trabajo seguras. AWS Comprender el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de operar cargas de AWS trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) puede ayudarlo a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso» : «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de gestionar cargas de trabajo seguras AWS . Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	iam-policy-no-stat ements-with-full-a ccess	Asegúrese de que las acciones de IAM se limiten únicament e a las acciones necesarias. Permitir que los usuarios tengan más privilegi os de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidades que debe administrar al abordar la operación de AWS cargas de trabajo seguras. Comprender el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantizar que las identidades correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidades humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicaciones. Se trata de miembros de su organización o usuarios externos	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidades que debe administrar al abordar la operación de cargas de trabajo seguras AWS . Comprender el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantizar que las identidades correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidades humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicaciones. Se trata de miembros de su organización o usuarios externos	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de operar AWS cargas de trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	secretsmanager-rot ation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencial mente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar cuando se trata de operar AWS cargas de trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	secretsmanager-sch eduled-rotation-su ccess-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribui do correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de operar cargas de AWS trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	secretsmanager-sec ret-periodic-rotation	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación periódica . La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar cuando se trata de operar AWS cargas de trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	secretsmanager-sec ret-unused	Si existen credencia les no utilizadas en AWS Secrets Manager, debe deshabilitar la opción and/or Eliminar las credenciales, ya que esto podría infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedFor Days (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de operar AWS cargas de trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	secretsmanager-usi ng-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenc iales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-2	¿Cómo se gestionan las identidades de las personas y las máquinas? Hay dos tipos de identidad es que hay que gestionar a la hora de operar AWS cargas de trabajo seguras. Comprende r el tipo de identidad que necesita para administrar y conceder el acceso le ayuda a garantiza r que las identidad es correctas tengan acceso a los recursos pertinentes en las condiciones adecuadas. Identidad es humanas: sus administradores, desarrolladores, operadores y usuarios finales necesitan una identidad para acceder a sus AWS entornos y aplicacio nes. Se trata de miembros de su organización o usuarios externos	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizad os para garantiza r que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomenda da de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven compromet idas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	con los que colabora y que interactú an con sus AWS recursos desde un navegador web, una aplicación cliente o herramientas interacti vas de línea de comandos. Identidad es de las máquinas: las aplicaciones de servicio, las herramientas operativas y las cargas de trabajo requieren una identidad para realizar solicitudes de AWS servicios, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su AWS entorno, como instancias de Amazon EC2 o funciones Lambda AWS . También se podrían administr ar identidades de máquina para las partes externas que necesiten acceso. Además, es posible		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que también tenga máquinas externas AWS que necesiten acceder a su AWS entorno.		
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegi o mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	ecs-containers-non privileged	Para ayudar a implementar el principio de privilegio mínimo, las definicio nes de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitad os los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegi os elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	ecs-containers-rea donly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegi o mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	efs-access-point-e nforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configura da en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros componentes deben acceder a cada componente o recurso de la carga de trabajo. Establezca una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autenticación y autorización adecuados.	iam-group-has-users-compruebe	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros componentes deben acceder a cada componente o recurso de la carga de trabajo. Establezca una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autenticación y autorización adecuados.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	iam-policy-no-stat ements-with-full-a ccess	Asegúrese de que las acciones de IAM se limiten únicament e a las acciones necesarias. Permitir que los usuarios tengan más privilegi os de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros componentes deben acceder a cada componente o recurso de la carga de trabajo. Establezca una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autenticación y autorización adecuados.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros componentes deben acceder a cada componente o recurso de la carga de trabajo. Establezca una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autenticación y autorización adecuados.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Los administradores, los usuarios finales u otros component es deben acceder a cada componente o recurso de la carga de trabajo. Establezc a una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autentica ción y autorización adecuados.	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Establezca controles comunes que restrinjan el acceso a todas las identidades de su organización. Por ejemplo, puedes restringir el acceso a AWS regiones específicas o impedir que tus operadores eliminen recursos comunes, como una función de IAM utilizada por tu equipo de seguridad central	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicamente a los recursos que requieran este tipo de acceso.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	s3- -bloques-periodico s account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictPublicBuck ets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	s3- bucket-level-publi c-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	secretsmanager-sec ret-unused	Si existen credencia les no utilizadas en AWS Secrets Manager, debe deshabilitar la opción and/or Eliminar las credenciales, ya que esto podría infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedFor Days (Config Default: 90). El valor real debe reflejar las políticas de su organización.
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	ssm-document-not-p ublic	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-3	¿Cómo se gestionan los permisos de las personas y las máquinas? Supervise continuamente los hallazgos que destaquen el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas únicament e a los recursos que requieran este tipo de acceso.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un objeto de un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-4	¿Cómo se detectan e investigan los eventos de seguridad ? Capture y analice los eventos a partir de registros y métricas para obtener una mejor visibilidad. Actúe ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	ec2- instance-multiple-eni-check	Esta regla comprueba si las instancias de Amazon Elastic Compute Cloud (Amazon EC2) tienen varias. ENIs Tener varias ENIs puede provocar instancias de doble host, es decir, instancias que tienen varias subredes. Esto puede añadir complejidad a la seguridad de la red e introducir rutas y accesos a la red no deseados.
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	account-level-public-accesss3- -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	waf-regional-rule-not-vacío	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencadenar un comportamiento no deseado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	waf-regional-rulegroup-not-vacío	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportamiento no deseado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-5	¿Cómo protege los recursos de su red? Cualquier carga de trabajo que tenga algún tipo de conectividad de red, ya sea a Internet o una red privada, requiere varios niveles de defensa para ayudar a protegerse de las amenazas externas e internas basadas en la red.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ecr-private-image-scanning-habilitado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ecs-container-insights-enabled	La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon Elastic Container Service (ECS) y sus AWS soluciones. Información de contenedores también proporciona información de diagnóstico, como, por ejemplo, errores de reinicio de contenedores, para ayudarlo a aislar problemas y solucionarlos rápidamente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2- instance-multiple-eni-check	Esta regla comprueba si las instancias de Amazon Elastic Compute Cloud (Amazon EC2) tienen varias. ENIs Tener varias ENIs puede provocar instancias de doble host, es decir, instancias que tienen varias subredes. Esto puede añadir complejidad a la seguridad de la red e introducir rutas y accesos a la red no deseados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2- -eni-periodic security-group-attached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-6	¿Cómo protege sus recursos de computación? Los recursos de computación de su carga de trabajo requieren varios niveles de defensa para protegerse de las amenazas externas e internas. Los recursos informáticos incluyen instancias EC2, contenedores, funciones AWS Lambda, servicios de bases de datos, dispositivos IoT y más.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	api-gw-cache-enabled-y cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	codebuild-project-s3 registros cifrados	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para AWS CodeBuild los registros almacenados en Amazon S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	s3- account-level-public-access -bloques-periodicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-8	¿Cómo protege sus datos en reposo? Proteja sus datos en reposo mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o mala gestión.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SEC-9	¿Cómo protege sus datos en tránsito? Proteja sus datos en tránsito mediante la implementación de varios controles para reducir el riesgo de acceso no autorizado o pérdida.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el pilar de seguridad AWS Well-Architected.

Prácticas operativas recomendadas para BCP y DR

Este paquete de conformidad contiene AWS Config reglas basadas en el BCP y el DR interno. AWS Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para BCP y DR.

Mejores prácticas operativas para BNM T RMi

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre la gestión de riesgos en tecnología (RMiT) de Bank Negara Malaysia (BNM) y las reglas de AWS Config gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles BNM RMi T. Un control BNM RMi T puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesario s para respaldar los controles criptográ ficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesario s para respaldar los controles criptográ ficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesario s para respaldar los controles criptográ ficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesario s para respaldar los controles criptográ ficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesario s para respaldar los controles criptográ ficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesarios para respaldar los controles criptográficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.18	Una institución financiera debe actuar con la debida diligencia y evaluar los controles criptográficos asociados a la tecnología utilizada para proteger la confidencialidad, la integridad, la autenticación, la autorización y el no rechazo de la información. Si una entidad financiera no genera sus propias claves de cifrado, debe adoptar las medidas adecuadas para garantizar que existan controles y procesos sólidos para administrar las claves de cifrado. Cuando ello implique basarse en evaluaciones de terceros, la entidad financiera deberá considerar si dicha confianza es coherente con la propensión y la tolerancia a	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	riesgos de la entidad financiera. La entidad financiera también debe prestar la debida atención a los recursos del sistema necesario s para respaldar los controles criptográ ficos y al riesgo de que se reduzca la visibilidad de los datos cifrados en el tráfico de red.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.20	Las instituciones financieras deben almacenar las claves criptográficas públicas en un certificado emitido por una autoridad de certificación en función del nivel de riesgo. Estos certificados asociados a los clientes deben ser emitidos por autoridades de certificación reconocidas. La entidad financiera debe garantizar que la aplicación de los protocolos de autenticación y firma que utilicen dichos certificados esté sujeta a una protección rigurosa, a fin de garantizar que el uso de las claves criptográficas privadas correspondientes a los certificados de usuario sea jurídicamente vinculante e irrefutable. La emisión inicial y la posterior	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	renovación de dichos certificados deben ser coherentes con las mejores prácticas de la industria y las legal/regulatory especific aciones aplicables.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.20	Las instituciones financieras deben almacenar las claves criptográficas públicas en un certificado emitido por una autoridad de certifica ción en función del nivel de riesgo. Estos certificados asociados a los clientes deben ser emitidos por autoridad es de certificación reconocidas. La entidad financier a debe garantiza r que la aplicación de los protocolos de autenticación y firma que utilicen dichos certificados esté sujeta a una protecció n rigurosa, a fin de garantizar que el uso de las claves criptográ ficas privadas correspondientes a los certificados de usuario sea jurídicam ente vinculante e irrefutable. La emisión inicial y la posterior	elbv2- acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	renovación de dichos certificados deben ser coherentes con las mejores prácticas de la industria y las legal/regulatory especific aciones aplicables.		
10.27	Una instituci ón financiera debe establece r mecanismos de monitoreo en tiempo real para realizar el seguimiento de la utilización de la capacidad y el rendimiento de los procesos y servicios clave. Estos mecanismos de supervisión deben ser capaces de proporcio nar alertas oportunas y procesables a los administradores.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automátic o de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibi lidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexione s o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.27	Una institución financiera debe establecer mecanismos de monitoreo en tiempo real para realizar el seguimiento de la utilización de la capacidad y el rendimiento de los procesos y servicios clave. Estos mecanismos de supervisión deben ser capaces de proporcionar alertas oportunas y procesables a los administradores.	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.27	Una institución financiera debe establecer mecanismos de monitoreo en tiempo real para realizar el seguimiento de la utilización de la capacidad y el rendimiento de los procesos y servicios clave. Estos mecanismos de supervisión deben ser capaces de proporcionar alertas oportunas y procesables a los administradores.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.27	Una institución financiera debe establecer mecanismos de monitoreo en tiempo real para realizar el seguimiento de la utilización de la capacidad y el rendimiento de los procesos y servicios clave. Estos mecanismos de supervisión deben ser capaces de proporcionar alertas oportunas y procesables a los administradores.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.27	Una institución financiera debe establecer mecanismos de monitoreo en tiempo real para realizar el seguimiento de la utilización de la capacidad y el rendimiento de los procesos y servicios clave. Estos mecanismos de supervisión deben ser capaces de proporcionar alertas oportunas y procesables a los administradores.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
10.27	Una institución financiera debe establecer mecanismos de monitoreo en tiempo real para realizar el seguimiento de la utilización de la capacidad y el rendimiento de los procesos y servicios clave. Estos mecanismos de supervisión deben ser capaces de proporcionar alertas oportunas y procesables a los administradores.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.27	Una institución financiera debe establecer mecanismos de monitoreo en tiempo real para realizar el seguimiento de la utilización de la capacidad y el rendimiento de los procesos y servicios clave. Estos mecanismos de supervisión deben ser capaces de proporcionar alertas oportunas y procesables a los administradores.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,27	Una institución financiera debe establecer mecanismos de monitoreo en tiempo real para realizar el seguimiento de la utilización de la capacidad y el rendimiento de los procesos y servicios clave. Estos mecanismos de supervisión deben ser capaces de proporcionar alertas oportunas y procesables a los administradores.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.27	Una institución financiera debe establecer mecanismos de monitoreo en tiempo real para realizar el seguimiento de la utilización de la capacidad y el rendimiento de los procesos y servicios clave. Estos mecanismos de supervisión deben ser capaces de proporcionar alertas oportunas y procesables a los administradores.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,34	Una institución financiera debe garantizar que los servicios de red de sus sistemas esenciales sean fiables y no cuenten con SPOF para proteger los sistemas esenciales contra posibles fallos de red y ciberamenazas.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,34	Una institución financiera debe garantizar que los servicios de red de sus sistemas esenciales sean fiables y no cuenten con SPOF para proteger los sistemas esenciales contra posibles fallos de red y ciberamenazas.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.35	Una institución financiera debe establecer procesos de monitoreo del ancho de banda de la red en tiempo real y las métricas correspondientes de resiliencia del servicio de red para detectar cualquier sobreutilización del ancho de banda y las interrupciones del sistema debidas a la congestión del ancho de banda y a los fallos de la red. Esto incluye el análisis del tráfico para detectar tendencias y anomalías.	api-gw-xray-enabled	AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicació n y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Asegúrese de que X-Ray esté habilitad o para que pueda ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a AWS los recursos descendentes, los microservicios, las bases de datos y la web HTTP. APIs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.35	Una institución financiera debe establecer procesos de monitoreo del ancho de banda de la red en tiempo real y las métricas correspondientes de resiliencia del servicio de red para detectar cualquier sobreutilización del ancho de banda y las interrupciones del sistema debidas a la congestión del ancho de banda y a los fallos de la red. Esto incluye el análisis del tráfico para detectar tendencias y anomalías.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.35	Una institución financiera debe establecer procesos de monitoreo del ancho de banda de la red en tiempo real y las métricas correspondientes de resiliencia del servicio de red para detectar cualquier sobreutilización del ancho de banda y las interrupciones del sistema debidas a la congestión del ancho de banda y a los fallos de la red. Esto incluye el análisis del tráfico para detectar tendencias y anomalías.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,35	Una institución financiera debe establecer procesos de monitoreo del ancho de banda de la red en tiempo real y las métricas correspondientes de resiliencia del servicio de red para detectar cualquier sobreutilización del ancho de banda y las interrupciones del sistema debidas a la congestión del ancho de banda y a los fallos de la red. Esto incluye el análisis del tráfico para detectar tendencias y anomalías.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,36	Una institución financiera debe garantizar que los servicios de red que respaldan los sistemas esenciales estén diseñados e implementados para garantizar la confidencialidad, integridad y disponibilidad de los datos.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
10.36	Una institución financiera debe garantizar que los servicios de red que respaldan los sistemas esenciales estén diseñados e implementados para garantizar la confidencialidad, integridad y disponibilidad de los datos.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,36	Una institución financiera debe garantizar que los servicios de red que respaldan los sistemas esenciales estén diseñados e implementados para garantizar la confidencialidad, integridad y disponibilidad de los datos.	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
10.36	Una institución financiera debe garantizar que los servicios de red que respaldan los sistemas esenciales estén diseñados e implementados para garantizar la confidencialidad, integridad y disponibilidad de los datos.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,36	Una institución financiera debe garantizar que los servicios de red que respaldan los sistemas esenciales estén diseñados e implementados para garantizar la confidencialidad, integridad y disponibilidad de los datos.	nlb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus balanceadores de carga de red (NLBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.38	Una institución financiera debe garantizar que se conserven suficient es registros de los dispositivos de red relevantes para las investigaciones y con fines forenses durante al menos tres años.	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizad os para garantiza r que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomenda da de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven compromet idas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	account-part-of-or ganizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantiza r que las cuentas cumplan con las normas. La falta de gobernanza centraliz ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	api-gw-cache-enabl ed-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	autoscaling-launch -config-public-ip- deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	backup-recovery-po int-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	cmk-backing-key-ro tation-habilitado	Habilite la rotación de claves para garantiza r que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	dynamodb-table-enc rypted-kms	Asegúrese de que el cifrado esté habilitad o para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenc iales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	efs-encrypted-check	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	elb 2- acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financiera debe implementar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgación y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapartes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	iam-user-group-mem bership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizac iones de acceso, ya que garantiza que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube aseguránd ose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	kms-cmk-not-schedu led-para su eliminaci ón	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programad as para su eliminaci ón en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financiera debe implementar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgación y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapartes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
10.51	Al utilizar los servicios en la nube, una institución financiera debe implementar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgación y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapartes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	opensearch-encrypt ed-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	opensearch-https-r equired	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	opensearch-node-to -node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financiera debe implementar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgación y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapartes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitad o para su clúster de Amazon Redshift. Puesto que puede haber datos confidenc iales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protecció n además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financiera debe implementar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgación y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapartes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	s3- -bloques-periódico s account-level-public-access	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictPublicBuck ets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	sagemaker-notebook -instance-kms-conf igurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	ssm-document-not-p ublic	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.51	Al utilizar los servicios en la nube, una institución financier a debe implement ar las medidas de seguridad adecuadas en relación con la información de los clientes y las contrapartes y los datos protegidos contra toda divulgaci ón y acceso no autorizados. Esto incluye conservar la propiedad, el control y la administración de todos los datos relacionados con la información de clientes y contrapar tes, los datos de propiedad y los servicios alojados en la nube, incluida la administración de las claves criptográficas pertinentes.	subnet-auto-assign-public-ip-deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizad os para garantiza r que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomenda da de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven compromet idas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	account-part-of-or ganizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantiza r que las cuentas cumplan con las normas. La falta de gobernanza centraliz ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) puede ayudarlo a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso» : «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	iam-user-group-mem bership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizac iones de acceso, ya que garantiza que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protecció n además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.52	Una institución financiera debe implementar una política de controles de acceso adecuada para la identific ación, autenticación y autorización de los usuarios (usuarios internos y externos, como los proveedores de servicios externos) . Esto debe abordar los controles de acceso a la tecnologí a tanto lógicos como físicos, que sean proporcionales al nivel de riesgo de acceso no autorizado a sus sistemas tecnológi cos.	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protecció n además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(b)(h)(i)	Al observar el párrafo 10.52, una institución financiera debe tener en cuenta los siguientes principios en su política de control de acceso: (b) emplear derechos de acceso con «privilegios mínimos» o sobre una base de «»need-to-have, cuando solo se concedan los permisos mínimos suficientes a los usuarios legítimos para desempeñar sus funciones; (h) limitar y controlar el intercambio de ID de usuario y contraseñas entre varios usuarios; e (i) controlar el uso de convenciones de nomenclatura de identificadores de usuario genéricos en favor de una mayor identificación personal IDs.	iam-root-access-key-check	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(b)	Al cumplir con el párrafo 10.52, una institución financier a debería tener en cuenta los siguiente s principios en su política de control de acceso: b) emplear derechos de acceso con el «mínimo privilegio» o utilizar el criterio de «need-to-have», concedien do únicamente los permisos mínimos suficientes a los usuarios legítimos para que desempeñe n sus funciones;	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(b)	Al cumplir con el párrafo 10.52, una institución financier a debería tener en cuenta los siguiente s principios en su política de control de acceso: (b) emplear derechos de acceso con el «mínimo privilegio» o utilizar una base de «need-to-have» en la que solo se concedan los permisos mínimos suficientes a los usuarios legítimos para que desempeñe n sus funciones;	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(b)	Al observar el párrafo 10.52, una institución financiera debería tener en cuenta los siguientes principios en su política de control del acceso: b) emplear derechos de acceso con «privilegios mínimos» o utilizar una base de «need-to-have» en la que solo se concedan los permisos mínimos suficientes a los usuarios legítimos para que desempeñen sus funciones;	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
10.53(b)	Al observar el párrafo 10.52, una instituci ón financiera debería tener en cuenta los siguientes principio s en su política de control de acceso: (b) emplear derechos de acceso con el «mínimo privilegio» o utilizar una base de «» need-to-have en la que solo se concedan los permisos mínimos suficientes a los usuarios legítimos para que desempeñe n sus funciones;	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(b)	Al cumplir con el párrafo 10.52, una institución financiera debería tener en cuenta los siguientes principios en su política de control de acceso: (b) emplear derechos de acceso con el «mínimo privilegio» o utilizar una base de «need-to-have» en la que solo se concedan los permisos mínimos suficientes a los usuarios legítimos para que desempeñen sus funciones;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(b)	Al observar el párrafo 10.52, una institución financiera debería tener en cuenta los siguientes principios en su política de control del acceso: b) emplear derechos de acceso con «privilegios mínimos» o utilizar una base de «need-to-have» en la que solo se concedan los permisos mínimos suficientes a los usuarios legítimos para que desempeñen sus funciones;	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso, ya que garantiza que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(b)	Al observar el párrafo 10.52, una institución financiera debería tener en cuenta los siguientes principios en su política de control de acceso: (b) emplear derechos de acceso con el «mínimo privilegio» o utilizar una base de «» need-to-have en la que solo se concedan los permisos mínimos suficientes a los usuarios legítimos para que desempeñen sus funciones;	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(c)(f)	Si observamos el párrafo 10.52, una institución financier a debe tener en cuenta los siguiente s principios en su política de control de acceso: c) emplear derechos de acceso de tiempo limitado que restrinjan el acceso a un período específico, incluidos los derechos de acceso concedidos a los proveedores de servicios; (f) adoptar una autenticación más rígida para las actividades esenciale s, incluido el acceso remoto.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(f)(h)	Si observamos el párrafo 10.52, una institución financier a debe tener en cuenta los siguiente s principios en su política de control de acceso: (f) adoptar una autenticación más rígida para las actividades esenciale s, incluido el acceso remoto; (h) limitar y controlar el intercamb io de ID de usuario y contraseñas entre varios usuarios.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(f)(h)	Si observamos el párrafo 10.54, una institución financiera debe tener en cuenta los siguientes principios en su política de control de acceso: (f) adoptar una autenticación más rígida para las actividades esenciales, incluido el acceso remoto; (h) limitar y controlar el intercambio de ID de usuario y contraseñas entre varios usuarios.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.53(f)(h)	Si observamos el párrafo 10.54, una institución financier a debe tener en cuenta los siguiente s principios en su política de control de acceso: (f) adoptar una autenticación más rígida para las actividades esenciale s, incluido el acceso remoto; (h) limitar y controlar el intercamb io de ID de usuario y contraseñas entre varios usuarios.	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protecció n además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,54	Una institución financiera debe emplear procesos de autenticación rígidos para garantizar la autenticidad de las identidades en uso. Los mecanismos de autenticación deberán estar en consonanc ia con la importanc ia de las funciones y adoptar al menos uno o más de estos tres factores básicos de autenticación: algo que el usuario sepa (como una contraseñ a o un PIN), algo que posea (como una tarjeta inteligen te o un dispositi vo de seguridad) y algo del usuario (por ejemplo, caracterí sticas biométricas, como una huella dactilar o un patrón de retina).	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,54	Una institución financiera debe emplear procesos de autenticación rígidos para garantizar la autenticidad de las identidades en uso. Los mecanismos de autenticación deberán estar en consonancia con la importancia de las funciones y adoptar al menos uno o más de estos tres factores básicos de autenticación: algo que el usuario sepa (como una contraseña o un PIN), algo que posea (como una tarjeta inteligente o un dispositivo de seguridad) y algo del usuario (por ejemplo, características biométricas, como una huella dactilar o un patrón de retina).	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,54	Una institución financiera debe emplear procesos de autenticación rígidos para garantizar la autenticidad de las identidades en uso. Los mecanismos de autenticación deberán estar en consonancia con la importancia de las funciones y adoptar al menos uno o más de estos tres factores básicos de autenticación: algo que el usuario sepa (como una contraseña o un PIN), algo que posea (como una tarjeta inteligente o un dispositivo de seguridad) y algo del usuario (por ejemplo, características biométricas, como una huella dactilar o un patrón de retina).	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.55	Las instituciones financieras deberán revisar y adaptar periódicamente sus prácticas en materia de contraseñas para mejorar la resiliencia frente a los ataques en constante evolución. Esto incluye la generación eficaz y segura de contraseñas. Deben existir los controles adecuados para comprobar la seguridad de las contraseñas creadas.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.56	Los métodos de autenticación que dependen de más de un factor suelen ser más difíciles de comprometer que un sistema de un solo factor. Por este motivo, se anima a las instituci ones financieras a diseñar e implement ar adecuadamente (especialmente en los sistemas de alto riesgo o de inicio de sesión único) la autenticación multifact or (MFA) más fiable y que disuaden más contra el fraude.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.56	Los métodos de autenticación que dependen de más de un factor suelen ser más difíciles de comprometer que un sistema de un solo factor. Por este motivo, se anima a las instituciones financieras a diseñar e implementar adecuadamente (especialmente en los sistemas de alto riesgo o de inicio de sesión único) la autenticación multifactor (MFA) más fiable y que disuaden más contra el fraude.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.56	Los métodos de autenticación que dependen de más de un factor suelen ser más difíciles de comprometer que un sistema de un solo factor. Por este motivo, se anima a las instituciones financieras a diseñar e implementar adecuadamente (especialmente en los sistemas de alto riesgo o de inicio de sesión único) la autenticación multifactor (MFA) más fiable y que disuaden más contra el fraude.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investiga ción. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódica mente de manera oportuna.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investiga ción. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódica mente de manera oportuna.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investiga ción. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódica mente de manera oportuna.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investiga ción. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódica mente de manera oportuna.	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investiga ción. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódica mente de manera oportuna.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso, ya que garantiza que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10,59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investiga ción. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódica mente de manera oportuna.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.59	Una institución financiera debe garantizar: a) que los controles de acceso a los sistemas de toda la empresa se administren y supervisen de forma eficaz; y b) que las actividades de los usuarios en los sistemas esenciales se registren para su auditoría e investigación. Los registros de actividad deben conservarse durante al menos tres años y revisarse periódicamente de manera oportuna.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.60	Para cumplir con el requisito establecido en el párrafo 10.59, las grandes instituci ones financieras deben: a) implement ar un sistema de administración de acceso por identidad para gestionar y supervisar eficazmen te el acceso de los usuarios a los sistemas de toda la empresa; y (b) implementar herramientas de auditoría automatiz adas para detectar cualquier anomalía.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.60	Para cumplir con el requisito establecido en el párrafo 10.61, las grandes instituciones financieras deben: a) implementar un sistema de administración de acceso por identidad para gestionar y supervisar eficazmente el acceso de los usuarios a los sistemas de toda la empresa; y (b) implementar herramientas de auditoría automatizadas para detectar cualquier anomalía.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.60	Para cumplir con el requisito establecido en el párrafo 10.61, las grandes instituciones financieras deben: a) implementar un sistema de administración de acceso por identidad para gestionar y supervisar eficazmente el acceso de los usuarios a los sistemas de toda la empresa; y (b) implementar herramientas de auditoría automatizadas para detectar cualquier anomalía.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.61	Una institución financiera debe garantizar que los sistemas críticos no se ejecuten en sistemas obsoletos con vulnerabi lidades de seguridad conocidas o en sistemas tecnológi cos end-of-life (EOL). En este sentido, una institución financier a debe asignar claramente las responsabilidades a las funciones identificadas: (a) para monitorea r e implementar continuamente las últimas versiones de parches de manera oportuna; y (b) identificar los sistemas tecnológi cos esenciales que se están aproximan do al EOL para seguir tomando medidas correctivas.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.1	Una institución financiera debe garantizar que los sistemas críticos no se ejecuten en sistemas obsoletos con vulnerabilidades de seguridad conocidas o en sistemas tecnológicos end-of-life (EOL). En este sentido, una institución financiera debe asignar claramente las responsabilidades a las funciones identificadas: (a) para monitorear e implementar continuamente las últimas versiones de parches de manera oportuna; y (b) identificar los sistemas tecnológicos esenciales que se están aproximando al EOL para seguir tomando medidas correctivas.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.1	Una institución financiera debe garantizar que los sistemas críticos no se ejecuten en sistemas obsoletos con vulnerabilidades de seguridad conocidas o en sistemas tecnológicos end-of-life (EOL). En este sentido, una institución financiera debe asignar claramente las responsabilidades a las funciones identificadas: (a) para monitorear e implementar continuamente las últimas versiones de parches de manera oportuna; y (b) identificar los sistemas tecnológicos esenciales que se están aproximando al EOL para seguir tomando medidas correctivas.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.1	Una institución financiera debe garantizar que los sistemas críticos no se ejecuten en sistemas obsoletos con vulnerabilidades de seguridad conocidas o en sistemas tecnológicos end-of-life (EOL). En este sentido, una institución financiera debe asignar claramente las responsabilidades a las funciones identificadas: (a) para monitorear e implementar continuamente las últimas versiones de parches de manera oportuna; y (b) identificar los sistemas tecnológicos esenciales que se están aproximando al EOL para seguir tomando medidas correctivas.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.61	Una institución financiera debe garantizar que los sistemas críticos no se ejecuten en sistemas obsoletos con vulnerabilidades de seguridad conocidas o en sistemas tecnológicos end-of-life (EOL). En este sentido, una institución financiera debe asignar claramente las responsabilidades a las funciones identificadas: (a) para monitorear e implementar continuamente las últimas versiones de parches de manera oportuna; y (b) identificar los sistemas tecnológicos esenciales que se están aproximando al EOL para seguir tomando medidas correctivas.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	api-gw-cache-enabl ed-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba si están habilitadas varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(a)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (a) la confidencialidad e integridad de la información y las transacciones de los clientes y las contrapartes.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(b)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (b) la fiabilidad de los servicios prestados a través de canales y dispositivos con una interrupción mínima de los servicios.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(b)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (b) la fiabilidad de los servicios prestados a través de canales y dispositivos con una interrupción mínima de los servicios.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
10.64(b)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (b) la fiabilidad de los servicios prestados a través de canales y dispositivos con una interrupción mínima de los servicios.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(b)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (b) la fiabilidad de los servicios prestados a través de canales y dispositivos con una interrupción mínima de los servicios.	nlb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus NetworkLoad balanceadores (NLBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(b)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (b) la fiabilidad de los servicios prestados a través de canales y dispositivos con una interrupción mínima de los servicios.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(b)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (b) la fiabilidad de los servicios prestados a través de canales y dispositivos con una interrupción mínima de los servicios.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(b)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (b) la fiabilidad de los servicios prestados a través de canales y dispositivos con una interrupción mínima de los servicios.	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(b)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (b) la fiabilidad de los servicios prestados a través de canales y dispositivos con una interrupción mínima de los servicios.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	api-gw-execution-logging-habilitada	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(d)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al prestar servicios digitales que garanticen lo siguiente: (d) un registro de auditoría suficiente y un monitoreo de las transacciones anómalas.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	dynamodb-resources-protected-by-plan de copias de seguridad	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identific ar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identificar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.64(e)	Una institución financiera debe implementar controles de seguridad tecnológicos rígidos al proporcionar servicios digitales que garanticen lo siguiente: (e) la capacidad de identific ar y volver al punto de recuperación antes de un incidente o interrupción del servicio.	s3- resources-protected-by-backup - plan	Para facilitar los procesos de respaldo de datos, asegúrese de que sus depósitos de Amazon Simple Storage Service (S3) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.7	Una institución financiera debe implementar herramientas eficaces para respaldar el monitoreo continuo y proactivo y la detección oportuna de actividades anómalas en su infraestr uctura tecnológica. El monitoreo debe alcanzar a todos los sistemas esenciale s, incluida la infraestr uctura de apoyo.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.7	Una institución financiera debe implementar herramientas eficaces para respaldar el monitoreo continuo y proactivo y la detección oportuna de actividades anómalas en su infraestr uctura tecnológica. El monitoreo debe alcanzar a todos los sistemas esenciale s, incluida la infraestr uctura de apoyo.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.8	Una institución financiera debe asegurarse de que sus operaciones de ciberseguridad prevengan y detecten continuamente cualquier posible compromiso de sus controles de seguridad o cualquier posible debilitamiento de su postura de seguridad. En el caso de las grandes instituciones financieras, esto debe incluir la realización de una evaluación trimestral de la vulnerabilidad de los componentes de la red externa e interna compatibles con todos los sistemas esenciales.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.8	Una institución financiera debe asegurarse de que sus operaciones de ciberseguridad prevengan y detecten continuamente cualquier posible compromiso de sus controles de seguridad o cualquier posible debilitamiento de su postura de seguridad. En el caso de las grandes instituciones financieras, esto debe incluir la realización de una evaluación trimestral de la vulnerabilidad de los componentes de la red externa e interna compatibles con todos los sistemas esenciales.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.18(c)(f)	El SOC debe poder desempeñar las siguientes funciones : (c) administrar las vulnerabilidades; (f) proporcionar conocimiento de la situación para detectar adversari os y amenazas, incluidos el análisis y las operacion es de inteligencia sobre amenazas, y el monitoreo de los indicadores de compromiso (IOC). Esto incluye un análisis avanzado del comportamiento para detectar el malware sin firmas ni archivos e identific ar las anomalías que puedan suponer una amenaza para la seguridad, incluso en los puntos de conexión y en las capas de red.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.18(c)(f)	El SOC debe poder desempeñar las siguientes funciones : (c) administrar las vulnerabilidades; (f) proporcionar conocimiento de la situación para detectar adversari os y amenazas, incluidos el análisis y las operacion es de inteligencia sobre amenazas, y el monitoreo de los indicadores de compromiso (IOC). Esto incluye un análisis avanzado del comportamiento para detectar el malware sin firmas ni archivos e identific ar las anomalías que puedan suponer una amenaza para la seguridad, incluso en los puntos de conexión y en las capas de red.	guardduty-non-arch ived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasifica ciones para determina r las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.18(c)(f)	El SOC debe poder desempeñar las siguientes funciones : (c) administrar las vulnerabilidades; (f) proporcionar conocimiento de la situación para detectar adversari os y amenazas, incluidos el análisis y las operacion es de inteligencia sobre amenazas, y el monitoreo de los indicadores de compromiso (IOC). Esto incluye un análisis avanzado del comportamiento para detectar el malware sin firmas ni archivos e identific ar las anomalías que puedan suponer una amenaza para la seguridad, incluso en los puntos de conexión y en las capas de red.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.1	Realizar una revisión periódica de la configuración y los ajustes de las reglas de todos los dispositi vos de seguridad. Utilizar herramientas automatizadas para revisar y monitorea r los cambios en la configuración y los ajustes de las reglas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.1	Realizar una revisión periódica de la configuración y los ajustes de las reglas de todos los dispositivos de seguridad. Utilizar herramientas automatizadas para revisar y monitorear los cambios en la configuración y los ajustes de las reglas.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.5(b)	Asegúrese de que los controles de seguridad de las conexiones de redes server-to-server externas incluyen lo siguiente: (b) el uso de túneles seguros, como Transport Layer Security (TLS) y Virtual Private Network (VPN) IPSec	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Appendix 5.5(b)	Asegúrese de que los controles de seguridad para las conexiones de redes server-to-server externas incluyan lo siguiente: (b) el uso de túneles seguros, como Transport Layer Security (TLS) y Virtual Private Network (VPN) IPSec	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.5(b)	Asegúrese de que los controles de seguridad de las conexiones de redes server-to-server externas incluyan lo siguiente: (b) el uso de túneles seguros, como los de seguridad de capa de transporte (TLS) y de red privada virtual (VPN) IPSec	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
Appendix 5.5(b)	Asegúrese de que los controles de seguridad para las conexiones de redes server-to-server externas incluyen lo siguiente: (b) el uso de túneles seguros, como Transport Layer Security (TLS) y Virtual Private Network (VPN) IPSec	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.5(b)	Asegúrese de que los controles de seguridad de las conexiones de redes server-to-server externas incluyan lo siguiente: (b) el uso de túneles seguros, como Transport Layer Security (TLS) y Virtual Private Network (VPN) IPSec	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
Appendix 5.5(b)	Asegúrese de que los controles de seguridad para las conexiones de redes server-to-server externas incluyan lo siguiente: (b) el uso de túneles seguros como Transport Layer Security (TLS) y Virtual Private Network (VPN) IPSec	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.5(c)	Asegúrese de que los controles de seguridad de las conexiones a redes server-to-server externas incluyan lo siguiente: (c) implementar servidores provisionales con defensas y protección perimetrales adecuadas, como un firewall, un IPS y un antivirus.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.5(c)	Asegúrese de que los controles de seguridad de las conexiones de red server-to-server externas incluyan lo siguiente: (c) implementar servidores provisionales con defensas y protección perimetrales adecuadas, como un firewall, un sistema IPS y un antivirus.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.5(c)	Asegúrese de que los controles de seguridad para las conexiones de redes server-to-server externas incluyan lo siguiente : (c) implementar servidores provision ales con defensas y protección perimetra les adecuadas, como un firewall, un IPS y un antivirus.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube aseguránd ose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.6	Asegúrese de que los controles de seguridad para el acceso remoto al servidor incluyan lo siguiente: (a) restrinja el acceso únicamente a los dispositivos de punto final reforzados y bloqueados; (b) utilice túneles seguros como TLS y VPN IPSec; (c) implemente un servidor de «puerta de enlace» con defensas y protección perimetrales adecuadas, como firewall, IPS y antivirus; y (d) cierre los puertos relevantes inmediatamente después de que caduque el acceso remoto.	alb-http-to-https-comprobar la redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.6	Asegúrese de que los controles de seguridad para el acceso remoto al servidor incluyan lo siguiente: (a) restrinja el acceso únicament e a los dispositivos de punto final protegido s y bloqueados; (b) utilice túneles seguros como TLS y VPN IPSec; (c) despliegu e un servidor de «puerta de enlace» con defensas y protección perimetra les adecuadas, como un firewall, un IPS y un antivirus; y (d) cierre los puertos pertinentes inmediata mente después de que caduque el acceso remoto.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.6	Asegúrese de que los controles de seguridad para el acceso remoto al servidor incluyan lo siguiente: (a) restrinja el acceso únicament e a los dispositivos de punto final reforzado s y bloqueados; (b) utilice túneles seguros como TLS y VPN IPSec; (c) implement e un servidor de «puerta de enlace» con defensas y protección perimetra les adecuadas, como firewall, IPS y antivirus; y (d) cierre los puertos relevante s inmediatamente después de que caduque el acceso remoto.	opensearch-https-r equired	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.6	Asegúrese de que los controles de seguridad para el acceso remoto al servidor incluyan lo siguiente: (a) restrinja el acceso únicament e a los dispositivos de punto final reforzado s y bloqueados; (b) utilice túneles seguros como TLS y VPN IPSec; (c) implement e un servidor de «puerta de enlace» con defensas y protección perimetra les adecuadas, como firewall, IPS y antivirus; y (d) cierre los puertos relevante s inmediatamente después de que caduque el acceso remoto.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.6	Asegúrese de que los controles de seguridad para el acceso remoto al servidor incluyen lo siguiente: (a) restrinja el acceso únicament e a los dispositivos de punto final protegido s y bloqueados; (b) utilice túneles seguros como TLS y VPN IPSec; (c) implement e un servidor de «puerta de enlace» con defensas y protección perimetra les adecuadas, como firewall, IPS y antivirus; y (d) cierre los puertos pertinent es inmediatamente después de que caduque el acceso remoto.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 5.6	Asegúrese de que los controles de seguridad para el acceso remoto al servidor incluyan lo siguiente: (a) restrinja el acceso únicament e a los dispositivos de punto final reforzado s y bloqueados; (b) utilice túneles seguros como TLS y VPN IPSec; (c) implement e un servidor de «puerta de enlace» con defensas y protección perimetra les adecuadas, como firewall, IPS y antivirus; y (d) cierre los puertos relevante s inmediatamente después de que caduque el acceso remoto.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube aseguránd ose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (a)	Una institución financiera debe diseñar una arquitectura de nube sólida y garantizar que dicho diseño cumpla con las normas internacionales pertinentes para la aplicación prevista.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (b)	Se alienta a las instituciones financieras a adoptar los principios de confianza cero para ofrecer una arquitectura ciberresiliente, adoptando una mentalidad de «asumir una infracción», defense-in-depth superponiendo la microsegmentación, los derechos de acceso deny-by-default «menos privilegiados» y realizando inspecciones exhaustivas y validándolas continuamente cuando proceda.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (b)	Se alienta a las instituciones financieras a adoptar los principios de confianza cero para ofrecer una arquitectura ciberresiliente, adoptando una mentalidad de «dar por sentado que se ha producido una infracción», combinando defense-in-depth la microsegmentación, los derechos de acceso deny-by-default «menos privilegiados» y realizando inspecciones exhaustivas y validándolas continuamente cuando proceda.	subnet-auto-assign-public-ip-disabled	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (b)	Se alienta a las instituciones financieras a adoptar los principios de confianza cero para ofrecer una arquitectura ciberresiliente, adoptando una mentalidad de «dar por sentado que se ha producido una infracción», combinando defense-in-depth la microsegmentación, los derechos de acceso con deny-by-default «menos privilegios» y realizando inspecciones exhaustivas y validándolas continuamente cuando proceda.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (b)	Se alienta a las instituciones financieras a adoptar los principios de confianza cero para ofrecer una arquitectura ciberresiliente, adoptando una mentalidad de «dar por sentado que se ha producido una infracción», combinando defense-in-depth la microsegmentación, los derechos de acceso con «menos privilegios» y realizando inspecciones exhaustivas y validándolas continuamente cuando proceda. deny-by-default	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (c)	Una institución financiera debe utilizar el enfoque de arquitectura de red más reciente y el concepto y las soluciones de diseño de red adecuados para administrar y monitorear la seguridad granular de la red y el suministr o centralizado de la red al administrar la complejidad del entorno de red en la nube.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (c)	Una institución financiera debe utilizar el enfoque de arquitectura de red más reciente y el concepto y las soluciones de diseño de red adecuados para administrar y monitorear la seguridad granular de la red y el suministr o centralizado de la red al administrar la complejidad del entorno de red en la nube.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
Appendix 10 Part B - 1 (d)	Una institución financiera debe establecer y utilizar canales de comunicac ión seguros y cifrados para migrar servidore s físicos, aplicacio nes o datos a las plataformas en la nube.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (d)	Una institución financiera debe establecer y utilizar canales de comunicación seguros y cifrados para migrar servidores físicos, aplicaciones o datos a las plataformas en la nube.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (f) i)	El uso cada vez mayor de las interfaces de programación de aplicaciones (API) por parte de las instituciones financieras para interconectarse con proveedores de servicios de aplicaciones externos podría aumentar la eficiencia en la prestación de nuevos servicios. Sin embargo, esto puede aumentar la superficie expuesta a ciberataques y cualquier mala gestión puede amplificar el impacto de un incidente de seguridad de la información. Una institución financiera debe asegurarse de estar sujeta a rigurosos mecanismos de gestión y control, entre los que APIs se incluyen los siguientes: i) APIs debe estar diseñada para ofrecer un servicio resiliente a fin de evitar el riesgo	api-gwv2- authorization-type-configured	Asegurarse de que la ruta de la API de Amazon API Gateway versión 2 tenga un tipo de autorización establecido para evitar el acceso no autorizado a los recursos de backend subyacentes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de puntos únicos de fallo y configurarse de forma segura con los controles de acceso adecuados;		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (f) ii)	El uso cada vez mayor de las interfaces de programación de aplicaciones (API) por parte de las instituciones financieras para interconectarse con proveedores de servicios de aplicaciones externos podría aumentar la eficiencia en la prestación de nuevos servicios. Sin embargo, esto puede aumentar la superficie expuesta a ciberataques y cualquier mala gestión puede amplificar el impacto de un incidente de seguridad de la información. Una institución financiera debe asegurarse de estar sujeta a rigurosos mecanismos de gestión y control, entre los que se incluyen los siguientes: ii) APIs debe ser rastreada y monitoreada para evitar los ciberataques con	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	medidas adecuadas de respuesta a los incidentes y ser desmanteladas oportunamente cuando ya no estén en uso. APIs		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 1 (f) ii)	El uso cada vez mayor de las interfaces de programación de aplicaciones (API) por parte de las instituciones financieras para interconectarse con proveedores de servicios de aplicaciones externos podría aumentar la eficiencia en la prestación de nuevos servicios. Sin embargo, esto puede aumentar la superficie expuesta a ciberataques y cualquier mala gestión puede amplificar el impacto de un incidente de seguridad de la información. Una institución financiera debe asegurarse de estar sujeta a rigurosos mecanismos de gestión y control, entre los que APIs se incluyen los siguientes: ii) APIs debe ser rastreada y supervisada contra los ciberataques con	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	medidas adecuadas de respuesta a los incidentes y ser desmantelada puntualmente cuando ya no esté en uso.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 2 (b) ii)	Una institución financiera debe aprovechar continuamente las capacidades mejoradas de la nube para mejorar la seguridad de los servicios en la nube y, entre otras cosas, se la anima a: ii) aplicar prácticas de infraestructura inmutables para la implementación de los servicios a fin de reducir el riesgo de error mediante la creación de un nuevo entorno con la última versión estable del software. El monitoreo continuo del entorno de nube debe incluir la automatización de la detección de cambios en la infraestructura inmutable para mejorar la revisión del cumplimiento y combatir la evolución de los ciberataques.	cloudformation-stack-notification-check	Para detectar cambios imprevistos en los AWS recursos subyacentes, asegúrese de que su CloudFormation pila esté configurada para enviar notificaciones de eventos a un tema de Amazon SNS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 3 (b) vi)	Una institución financiera debe garantizar que se configuren, protejan y monitoree n adecuadamente las imágenes de las máquinas virtuales y los contenedo res. Esto incluye lo siguiente: vi) las imágenes almacenad as están sujetas a un control de seguridad para evitar que se produzcan cambios o accesos no autorizad os.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (a) i)	Como parte de una capacidad de recuperación efectiva, las instituciones financieras deben garantizar que los procedimientos de copia de seguridad y recuperación existentes se extiendan a los servicios en la nube, lo que incluye lo siguiente: i) definir y formalizar la estrategia de copia de seguridad y recuperación en la fase de planificación de la adopción de la nube.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (a) i)	Como parte de una capacidad de recuperación efectiva, las instituciones financieras deben garantizar que los procedimientos de copia de seguridad y recuperación existentes se extiendan a los servicios en la nube, lo que incluye lo siguiente: i) definir y formalizar la estrategia de copia de seguridad y recuperación en la fase de planificación de la adopción de la nube.	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (a) i)	Como parte de una capacidad de recuperación efectiva, las instituciones financieras deben garantizar que los procedimientos de copia de seguridad y recuperación existentes se extiendan a los servicios en la nube, lo que incluye lo siguiente: i) definir y formalizar la estrategia de copia de seguridad y recuperación en la fase de planificación de la adopción de la nube.	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (a) i)	Como parte de una capacidad de recuperación efectiva, las instituciones financieras deben garantizar que los procedimientos de copia de seguridad y recuperación existentes se extiendan a los servicios en la nube, lo que incluye lo siguiente: i) definir y formalizar la estrategia de copia de seguridad y recuperación en la fase de planificación de la adopción de la nube.	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (a) i)	Como parte de una capacidad de recuperación efectiva, las instituciones financieras deben garantizar que los procedimientos de copia de seguridad y recuperación existentes se extiendan a los servicios en la nube, lo que incluye lo siguiente: i) definir y formalizar la estrategia de copia de seguridad y recuperación en la fase de planificación de la adopción de la nube.	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (a) i)	Como parte de una capacidad de recuperación efectiva, las instituciones financieras deben garantizar que los procedimientos de copia de seguridad y recuperación existentes se extiendan a los servicios en la nube, lo que incluye lo siguiente: i) definir y formalizar la estrategia de copia de seguridad y recuperación en la fase de planificación de la adopción de la nube.	plan s3 resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus depósitos de Amazon Simple Storage Service (S3) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (b)	Una institución financiera debe garantizar que los procedimientos de copia de seguridad y restauración se prueben periódica mente para validar las capacidades de recuperación. La frecuencia de los procedimientos de copia de seguridad debe ser proporcio nal a la criticida d del sistema y al objetivo de punto de recuperación (RPO) del sistema. La institución financiera debe tomar medidas correctivas a la mayor brevedad posible en caso de que las copias de seguridad no se realicen correctam ente.	backup-plan-min-fr equency-and-min-re tention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) y requiredF requencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (c) i)	Una institución financiera debe garantizar un respaldo y una recuperación suficientes de la máquina virtual y el contenedor, incluidos los ajustes de configuración de respaldo (para IaaS y PaaS, cuando correspondiente), que incluyen lo siguiente: i) garantizar la capacidad de restaurar una máquina virtual y un contenedor point-in-time según lo especificado en los objetivos de recuperación empresarial;	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (d) i)	Una institución financiera debe evaluar los requisito s de resiliencia de los servicios en la nube e identificar las medidas adecuadas que estén en consonancia con la criticidad del sistema, a fin de garantiza r la disponibilidad del servicio en los escenarios extremada mente adversos. Las instituciones financieras deben considerar aplicar un enfoque basado en el riesgo y adoptar progresivamente los controles de mitigació n adecuados para garantizar la disponibi lidad de los servicios y mitigar el riesgo de concentración. Entre las opciones viables se encuentra n: i) aprovechar las características de alta disponibilidad y redundancia de los servicios en la nube	autoscaling-multiple-az	Para garantizar una alta disponibilidad, asegúrese de que su grupo de escalado automático esté configurado para abarcar varias zonas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	para garantizar que los centros de datos de producción tengan capacidad redundant e en las diferentes zonas de disponibi lidad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (d) i)	Una institución financiera debe evaluar los requisito s de resiliencia de los servicios en la nube e identificar las medidas adecuadas que estén en consonancia con la criticidad del sistema, a fin de garantiza r la disponibilidad del servicio en los escenarios extremada mente adversos. Las instituciones financieras deben considerar aplicar un enfoque basado en el riesgo y adoptar progresivamente los controles de mitigació n adecuados para garantizar la disponibi lidad de los servicios y mitigar el riesgo de concentración. Entre las opciones viables se encuentra n: i) aprovechar las características de alta disponibilidad y redundancia de los servicios en la nube	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantiza r una alta disponibi lidad, asegúrese de que su ELB tenga instancias registrad as de varias zonas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	para garantizar que los centros de datos de producción tengan capacidad redundante en las diferentes zonas de disponibilidad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (d) i)	Una institución financiera debe evaluar los requisito s de resiliencia de los servicios en la nube e identificar las medidas adecuadas que estén en consonancia con la criticidad del sistema, a fin de garantiza r la disponibilidad del servicio en los escenarios extremada mente adversos. Las instituciones financieras deben considerar aplicar un enfoque basado en el riesgo y adoptar progresivamente los controles de mitigació n adecuados para garantizar la disponibi lidad de los servicios y mitigar el riesgo de concentración. Entre las opciones viables se encuentra n: i) aprovechar las características de alta disponibilidad y redundancia de los servicios en la nube	lambda-vpc-multi-az-comprobar	Si su función AWS Lambda está configurada para conectarse a una nube privada virtual (VPC) de su cuenta, implemente la función AWS Lambda en al menos dos zonas de disponibilidad diferentes para asegurarse de que su función esté disponibl e para procesar eventos en caso de una interrupción del servicio en una sola zona.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	para garantizar que los centros de datos de producción tengan capacidad redundante en las diferentes zonas de disponibilidad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (d) i)	Una institución financiera debe evaluar los requisitos de resiliencia de los servicios en la nube e identificar las medidas adecuadas que estén en consonancia con la criticidad del sistema, a fin de garantizar la disponibilidad del servicio en los escenarios extremadamente adversos. Las instituciones financieras deben considerar aplicar un enfoque basado en el riesgo y adoptar progresivamente los controles de mitigación adecuados para garantizar la disponibilidad de los servicios y mitigar el riesgo de concentración. Entre las opciones viables se encuentran: i) aprovechar las características de alta disponibilidad y redundancia de los servicios en la nube	nlb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus NetworkLoad balanceadores (NLBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	para garantizar que los centros de datos de producción tengan capacidad redundante en las diferentes zonas de disponibilidad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (d) i)	Una institución financiera debe evaluar los requisito s de resiliencia de los servicios en la nube e identificar las medidas adecuadas que estén en consonancia con la criticidad del sistema, a fin de garantiza r la disponibilidad del servicio en los escenarios extremada mente adversos. Las instituciones financieras deben considerar aplicar un enfoque basado en el riesgo y adoptar progresivamente los controles de mitigació n adecuados para garantizar la disponibi lidad de los servicios y mitigar el riesgo de concentración. Entre las opciones viables se encuentra n: i) aprovechar las características de alta disponibilidad y redundancia de los servicios en la nube	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relationa l Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenad os. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	para garantizar que los centros de datos de producción tengan capacidad redundant e en las diferentes zonas de disponibi lidad.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 5 (d) i)	Una institución financiera debe evaluar los requisito s de resiliencia de los servicios en la nube e identificar las medidas adecuadas que estén en consonancia con la criticidad del sistema, a fin de garantiza r la disponibilidad del servicio en los escenarios extremada mente adversos. Las instituciones financieras deben considerar aplicar un enfoque basado en el riesgo y adoptar progresivamente los controles de mitigació n adecuados para garantizar la disponibi lidad de los servicios y mitigar el riesgo de concentración. Entre las opciones viables se encuentra n: i) aprovechar las características de alta disponibilidad y redundancia de los servicios en la nube	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	para garantizar que los centros de datos de producción tengan capacidad redundant e en las diferentes zonas de disponibi lidad.		la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidenc ialidad e integridad de los datos sensibles almacenados en la nube.	api-gw-cache-enabl ed-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba si están habilitadas varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidenc ialidad e integridad de los datos sensibles almacenados en la nube.	eks-secrets-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que los clústeres de Amazon Elastic Kubernetes Service (EKS) estén configura dos para cifrar los secretos de Kubernetes. Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidenc ialidad e integridad de los datos sensibles almacenados en la nube.	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (a)	Una institución financiera debe implementar técnicas de cifrado adecuadas y pertinentes para proteger la confidencialidad e integridad de los datos sensibles almacenados en la nube.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (d)	A medida que aumenta el uso de la nube, la administración de numerosas claves de cifrado utilizadas para proteger los datos se ha vuelto más compleja y puede suponer nuevos desafíos para las instituciones financieras. Una institución financiera debe adoptar un enfoque integral y centralizado de la administración de claves, que incluya el uso de un sistema de administración de claves centralizado que pueda gestionar la generación, el almacenamiento y la distribución de claves de forma segura y escalable.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 8 (d)	A medida que aumenta el uso de la nube, la administración de numerosas claves de cifrado utilizadas para proteger los datos se ha vuelto más compleja y puede suponer nuevos desafíos para las instituciones financieras. Una institución financiera debe adoptar un enfoque integral y centralizado de la administración de claves, que incluya el uso de un sistema de administración de claves centralizado que pueda gestionar la generación, el almacenamiento y la distribución de claves de forma segura y escalable.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 9 (a) ii)	El plano de administración es una diferencia de seguridad de claves entre la infraestructura tradicional y la computación en la nube, donde se admite el acceso remoto de forma predeterminada. Esta capa de acceso podría ser propensa a sufrir ciberataques, lo que pondría en peligro la integridad de toda la implementación en la nube. Por ello, las instituciones financieras deben garantizar el uso de controles rígidos para acceder al plano de administración, que pueden incluir lo siguiente: ii) implementar la autenticación multifactor (MFA) y los privilegios mínimos, como una contraseña segura, un token de software,	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	una herramienta de gestión de acceso con privilegios y funciones de verificación y fabricación.		), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 9 (a) ii)	El plano de administración es una diferencia de seguridad de claves entre la infraestructura tradicional y la computación en la nube, donde se admite el acceso remoto de forma predeterminada. Esta capa de acceso podría ser propensa a sufrir ciberataques, lo que pondría en peligro la integridad de toda la implementación en la nube. Por ello, las instituciones financieras deben garantizar el uso de controles rígidos para acceder al plano de administración, que pueden incluir lo siguiente: ii) implementar la autenticación multifactor (MFA) y los privilegios mínimos, como una contraseña segura, un token de software,	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	una herramienta de gestión de acceso con privilegios y funciones de verificación y fabricación.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 9 (a) ii)	El plano de administración es una diferencia de seguridad de claves entre la infraestructura tradicional y la computación en la nube, donde se admite el acceso remoto de forma predeterminada. Esta capa de acceso podría ser propensa a sufrir ciberataques, lo que pondría en peligro la integridad de toda la implementación en la nube. Por ello, las instituciones financieras deben garantizar el uso de controles rígidos para acceder al plano de administración, que pueden incluir lo siguiente: ii) implementar la autenticación multifactor (MFA) y los privilegios mínimos, como una contraseña segura, un token de software,	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	una herramienta de gestión de acceso con privilegios y funciones de verificación y fabricación.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 9 (a) ii)	El plano de administración es una diferencia de seguridad de claves entre la infraestructura tradicional y la computación en la nube, donde se admite el acceso remoto de forma predeterminada. Esta capa de acceso podría ser propensa a sufrir ciberataques, lo que pondría en peligro la integridad de toda la implementación en la nube. Por ello, las instituciones financieras deben garantizar el uso de controles rígidos para acceder al plano de administración, que pueden incluir lo siguiente: ii) implementar la autenticación multifactor (MFA) y los privilegios mínimos, como una contraseña segura, un token de software,	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	una herramienta de gestión de acceso con privilegios y funciones de verificación y fabricación.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 9 (a) iii)	El plano de administración es una diferencia de seguridad de claves entre la infraestructura tradicional y la computación en la nube, donde se admite el acceso remoto de forma predeterminada. Esta capa de acceso podría ser propensa a sufrir ciberataques, lo que pondría en peligro la integridad de toda la implementación en la nube. Por ello, las instituciones financieras deben garantizar el uso de controles estrictos para acceder al plano de gestión, que pueden incluir lo siguiente: iii) emplear una asignación pormenorizada de los derechos para los usuarios con privilegios.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 9 (a) iii)	El plano de administración es una diferencia de seguridad de claves entre la infraestructura tradicional y la computación en la nube, donde se admite el acceso remoto de forma predeterminada. Esta capa de acceso podría ser propensa a sufrir ciberataques, lo que pondría en peligro la integridad de toda la implementación en la nube. Por ello, las instituciones financieras deben garantizar el uso de controles estrictos para acceder al plano de gestión, que pueden incluir lo siguiente: iii) emplear una asignación pormenorizada de los derechos para los usuarios con privilegios.	iam-user-no-policies-compruebe	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 9 (a) iv)	El plano de administración es una diferencia de seguridad de claves entre la infraestructura tradicional y la computación en la nube, donde se admite el acceso remoto de forma predeterminada. Esta capa de acceso podría ser propensa a sufrir ciberataques, lo que pondría en peligro la integridad de toda la implementación en la nube. Por ello, las instituciones financieras deben garantizar el uso de controles estrictos para acceder al plano de gestión, que pueden incluir lo siguiente: iv) llevar a cabo un monitoreo continuo de las actividades realizadas por los usuarios con privilegios.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 9 (a) iv)	El plano de administración es una diferencia de seguridad de claves entre la infraestructura tradicional y la computación en la nube, donde se admite el acceso remoto de forma predeterminada. Esta capa de acceso podría ser propensa a sufrir ciberataques, lo que pondría en peligro la integridad de toda la implementación en la nube. Por ello, las instituciones financieras deben garantizar el uso de controles estrictos para acceder al plano de gestión, que pueden incluir lo siguiente: iv) llevar a cabo un monitoreo continuo de las actividades realizadas por los usuarios con privilegios.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 12 (a)	Una institución financiera debe proteger los datos alojados en los servicios en la nube, tal como se exige en la sección sobre prevenció n de pérdidas de datos (párrafos 11.14 a 11.16) de este documento de política, incluida la ampliación del espacio de los puntos de conexión si la institución financier a permite que su personal utilice sus propios dispositivos para acceder a los datos confidenciales.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 12 (a)	Una institución financiera debe proteger los datos alojados en los servicios en la nube, tal como se exige en la sección sobre prevenció n de pérdidas de datos (párrafos 11.14 a 11.16) de este documento de política, incluida la ampliación del espacio de los puntos de conexión si la institución financier a permite que su personal utilice sus propios dispositivos para acceder a los datos confidenciales.	macie-status-check	Amazon Macie es un servicio de seguridad y privacidad de los datos completam ente administrado que utiliza el machine learning y la coinciden cia de patrones para descubrir y ayudar a proteger los datos confidenciales en los buckets de Amazon Simple Storage Service (Amazon S3).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 14 (c) i)	Al desarrollar su CIRP, una institución financiera debe considerar las siguientes medidas adicionales: i) mejorar su capacidad para detectar incidentes de infracción de la seguridad a fin de lograr una gestión eficaz de los incidentes, incluida la capacidad de detectar la filtración de datos en la web oscura.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Appendix 10 Part B - 14 (c) i)	Al desarrollar su CIRP, una institución financiera debe considerar las siguientes medidas adicionales: i) mejorar su capacidad para detectar incidentes de infracción de la seguridad a fin de lograr una gestión eficaz de los incidentes, incluida la capacidad de detectar la filtración de datos en la web oscura.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para BNM T. RMi

Prácticas operativas recomendadas para el Perfil medio de control de la nube del Centro Canadiense de Ciberseguridad (CCCS)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el perfil de control en la nube mediana del Centro Canadiense de Ciberseguridad (CCCS) y las reglas de Config AWS administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles del perfil de control de CCCS Medium Cloud. Un control de Perfil medio de control de la nube del CCCS se puede relacionar con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(1)	AC-2(1) Administración de cuentas | Sistema automatizado de administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(3)	AC-2(3) Administración de cuentas | Deshabilitación de cuentas inactivas	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(3)	AC-2(3) Administración de cuentas | Deshabilitación de cuentas inactivas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(4)	AC-2(4) Administración de cuentas | Acciones de auditoría automatizadas	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
CCCS-fPBMM-AC-2(4)	AC-2(4) Administración de cuentas | Acciones de auditoría automatizadas	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(4)	AC-2(4) Administración de cuentas | Acciones de auditoría automatizadas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(4)	AC-2(4) Administración de cuentas | Acciones de auditoría automatizadas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(4)	AC-2(4) Administración de cuentas | Acciones de auditoría automatizadas	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(4)	AC-2(4) Administración de cuentas | Acciones de auditoría automatizadas	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2(4)	AC-2(4) Administración de cuentas | Acciones de auditoría automatizadas	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.A	AC-2.A Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.B	AC-2.B Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.C	AC-2.C Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.D	AC-2.D Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.E	AC-2.E Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.F	AC-2.F Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.G	AC-2.G Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.H	AC-2.H Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.I	AC-2.I Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.J	AC-2.J Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-2.K	AC-2.K Administración de cuentas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-3.A	AC-3.A Aplicación de normas de acceso	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4(21)	AC-4(21) Control del flujo de información | Separación física y lógica de los flujos de información	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-AC-4(21)	AC-4(21) Control del flujo de información | Separación física y lógica de los flujos de información	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4(21)	AC-4(21) Control del flujo de información | Separación física y lógica de los flujos de información	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4(21)	AC-4(21) Control del flujo de información | Separación física y lógica de los flujos de información	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4(21)	AC-4(21) Control del flujo de información | Separación física y lógica de los flujos de información	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-AC-4(21)	AC-4(21) Control del flujo de información | Separación física y lógica de los flujos de información	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4(21)	AC-4(21) Control del flujo de información | Separación física y lógica de los flujos de información	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-AC-4(21)	AC-4(21) Control del flujo de información | Separación física y lógica de los flujos de información	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4(21)	AC-4(21) Control del flujo de información | Separación física y lógica de los flujos de información	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-4.A	AC-4.A Aplicación del flujo de información	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-5.A	AC-5.A Separación de funciones	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-5.A	AC-5.A Separación de funciones	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-5.A	AC-5.A Separación de funciones	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-5.A	AC-5.A Separación de funciones	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-5.A	AC-5.A Separación de funciones	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio mínimo | Autorización de acceso a las funciones de seguridad	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio mínimo | Autorización de acceso a las funciones de seguridad	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio mínimo | Autorización de acceso a las funciones de seguridad	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio mínimo | Autorización de acceso a las funciones de seguridad	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio mínimo | Autorización de acceso a las funciones de seguridad	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio mínimo | Acceso sin privilegios para funciones no relacionadas con la seguridad	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio mínimo | Acceso sin privilegios para funciones no relacionadas con la seguridad	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio mínimo | Acceso sin privilegios para funciones no relacionadas con la seguridad	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio mínimo | Acceso sin privilegios para funciones no relacionadas con la seguridad	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio mínimo | Acceso sin privilegios para funciones no relacionadas con la seguridad	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(5)	AC-6(5) Privilegio mínimo | Cuentas con privilegios	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(5)	AC-6(5) Privilegio mínimo | Cuentas con privilegios	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(5)	AC-6(5) Privilegio mínimo | Cuentas con privilegios	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(5)	AC-6(5) Privilegio mínimo | Cuentas con privilegios	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio mínimo | Auditoría del uso de las funciones con privilegios	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio mínimo | Auditoría del uso de las funciones con privilegios	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio mínimo | Auditoría del uso de las funciones con privilegios	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio mínimo | Auditoría del uso de las funciones con privilegios	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio mínimo | Auditoría del uso de las funciones con privilegios	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio mínimo | Auditoría del uso de las funciones con privilegios	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio mínimo | Auditoría del uso de las funciones con privilegios	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegio mínimo | Prohibición de ejecutar funciones con privilegios a los usuarios sin privilegios	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegio mínimo | Prohibición de ejecutar funciones con privilegios a los usuarios sin privilegios	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegio mínimo | Prohibición de ejecutar funciones con privilegios a los usuarios sin privilegi os	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegio mínimo | Prohibición de ejecutar funciones con privilegios a los usuarios sin privilegios	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegio mínimo | Prohibición de ejecutar funciones con privilegios a los usuarios sin privilegios	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio mínimo	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(1)	AC-17(1) Acceso remoto | Monitoreo y control automatizados	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(2)	AC-17(2) Acceso remoto | Protección de la confidencialidad e integridad mediante el cifrado	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-AC-17(2)	AC-17(2) Acceso remoto | Protección de la confidencialidad e integridad mediante el cifrado	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(2)	AC-17(2) Acceso remoto | Protección de la confidencialidad e integridad mediante el cifrado	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(2)	AC-17(2) Acceso remoto | Protección de la confidencialidad e integridad mediante el cifrado	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-AC-17(2)	AC-17(2) Acceso remoto | Protección de la confidencialidad e integridad mediante el cifrado	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(2)	AC-17(2) Acceso remoto | Protección de la confidencialidad e integridad mediante el cifrado	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(3)	AC-17(3) Acceso remoto | Puntos de control de acceso administrados	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(4)	AC-17(4) Acceso remoto | Comandos privilegiados y acceso	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(4)	AC-17(4) Acceso remoto | Comandos privilegiados y acceso	mfa-enabled-for-iam-acceso desde la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17(4)	AC-17(4) Acceso remoto | Comandos privilegiados y acceso	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.A	AC-17.A Acceso remoto	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.AA	AC-17.AA Acceso remoto	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AC-17.B	AC-17.B Acceso remoto	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.A	AU-2.A Eventos de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.B	AU-2.B Eventos de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.C	AU-2.C Eventos de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-2.D	AU-2.D Eventos de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenido de los registros de auditoría | Información de auditoría adicional	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenido de los registros de auditoría | Información de auditoría adicional	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenido de los registros de auditoría | Información de auditoría adicional	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenido de los registros de auditoría | Información de auditoría adicional	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenido de los registros de auditoría | Información de auditoría adicional	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenido de los registros de auditoría | Información de auditoría adicional	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenido de los registros de auditoría | Información de auditoría adicional	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenido de los registros de auditoría | Información de auditoría adicional	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-3.A	AU-3.A Contenido de los registros de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-5.A	AU-5.A Respuesta a los fallos en el procesamiento de la auditoría	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-5.B	AU-5.B Respuesta a los fallos en el procesamiento de la auditoría	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisión, análisis e informes de auditoría | Integración de procesos	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisión, análisis e informes de auditoría | Integración de procesos	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisión, análisis e informes de auditoría | Integración de procesos	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisión, análisis e informes de auditoría | Integración de procesos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisión, análisis e informes de auditoría | Integración de procesos	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisión, análisis e informes de auditoría | Integración de procesos	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlacionar repositorios de auditoría	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlacionar repositorios de auditoría	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlaci onar repositorios de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlacionar repositorios de auditoría	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlacionar repositorios de auditoría	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlacionar repositorios de auditoría	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlacionar repositorios de auditoría	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlaci onar repositorios de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlaci onar repositorios de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlacionar repositorios de auditoría	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlaci onar repositorios de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlacionar repositorios de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlaci onar repositorios de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlaci onar repositorios de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisión, análisis e informes de auditoría | Correlacionar repositorios de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-7(1)	AU-7(1) Reducción de auditorías y generación de informes | Procesamiento automático	cloud-trail-cloud-watch-registros activados	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-8.B	AU-8.B Marcas temporales	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-9(2)	AU-9(2) Protección de la información de auditoría | Copia de seguridad de las auditorías en sistemas o componentes físicos separados	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-AU-9(2)	AU-9(2) Protección de la información de auditoría | Copia de seguridad de las auditorías en sistemas o componentes físicos separados	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-9(2)	AU-9(2) Protección de la información de auditoría | Copia de seguridad de las auditorías en sistemas o componentes físicos separados	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.
CCCS-fPBMM-AU-9.A	AU-9.A Protección de la información de auditoría	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-9.A	AU-9.A Protección de la información de auditoría	cloud-trail-log-file-habilitado para validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-9.A	AU-9.A Protección de la información de auditoría	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
CCCS-fPBMM-AU-11.A	AU-11.A Retención de los registros de auditoría	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-11.B	AU-11.B Retención de los registros de auditoría	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-11.C	AU-11.C Retención de los registros de auditoría	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.A	AU-12.A Generación de auditorías	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-AU-12.C	AU-12.C Generación de auditorías	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear las no utilizadas EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconexiones del sistema | Restricciones en las conexiones de redes externas	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	api-gw-xray-enabled	AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Asegúrese de que X-Ray esté habilitado para que pueda ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a AWS los recursos descendentes, los microservicios, las bases de datos y la web HTTP. APIs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.A	CA-7.A Monitoreo continuo	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	api-gw-xray-enabled	AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Asegúrese de que X-Ray esté habilitado para que pueda ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a AWS los recursos descendentes, los microservicios, las bases de datos y la web HTTP. APIs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear los no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.B	CA-7.B Monitoreo continuo	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	api-gw-xray-enabled	AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Asegúrese de que X-Ray esté habilitado para que pueda ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a AWS los recursos descendentes, los microservicios, las bases de datos y la web HTTP. APIs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear los no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.C	CA-7.C Monitoreo continuo	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	api-gw-xray-enabled	AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Asegúrese de que X-Ray esté habilitado para que pueda ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a AWS los recursos descendentes, los microservicios, las bases de datos y la web HTTP. APIs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear los no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.D	CA-7.D Monitoreo continuo	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	api-gw-xray-enabled	AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Asegúrese de que X-Ray esté habilitado para que pueda ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a AWS los recursos descendentes, los microservicios, las bases de datos y la web HTTP. APIs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear los no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.E	CA-7.E Monitoreo continuo	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	api-gw-xray-enabled	AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicació n y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Asegúrese de que X-Ray esté habilitad o para que pueda ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a AWS los recursos descendentes, los microservicios, las bases de datos y la web HTTP. APIs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear los no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.F	CA-7.F Monitoreo continuo	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	api-gw-xray-enabled	AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Asegúrese de que X-Ray esté habilitado para que pueda ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a AWS los recursos descendentes, los microservicios, las bases de datos y la web HTTP. APIs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear los no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-7.G	CA-7.G Monitoreo continuo	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CA-9.A	CA-9.A Conexiones internas del sistema	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-2.A	CM-2.A Configuración de referencia	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-2.A	CM-2.A Configuración de referencia	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-2.A	CM-2.A Configuración de referencia	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-2.A	CM-2.A Configuración de referencia	ec-2 volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-2.A	CM-2.A Configuración de referencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-2.A	CM-2.A Configuración de referencia	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-2.A	CM-2.A Configuración de referencia	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.A	CM-3.A Control de cambios de la configuración	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.A	CM-3.A Control de cambios de la configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.B	CM-3.B Control de cambios de la configuración	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.B	CM-3.B Control de cambios de la configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.C	CM-3.C Control de cambios de la configuración	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.C	CM-3.C Control de cambios de la configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.D	CM-3.D Control de cambios de la configuración	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.D	CM-3.D Control de cambios de la configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.E	CM-3.E Control de cambios de la configuración	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.E	CM-3.E Control de cambios de la configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.F	CM-3F Control de cambios de la configuración	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.F	CM-3F Control de cambios de la configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.G	CM-3.G Control de cambios de la configuración	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-3.G	CM-3.G Control de cambios de la configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(1)	CM-5(1) Restricciones de acceso para realizar cambios | Control y auditoría automatizados del acceso	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5(5)	CM-5(5) Restricciones de acceso para realizar cambios | Limitar los privilegios operativos o de producción	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms:descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-5.A	CM-5.A Restricciones de acceso para realizar cambios	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6(1)	CM-6(1) Opciones de configura ción | Administr ación centraliz ada automatiz ada, aplicaciones y verificación	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6(1)	CM-6(1) Opciones de configura ción | Administr ación centraliz ada automatiz ada, aplicaciones y verificación	ec2- -check managedinstance-as sociation-compliance-status	Use AWS Systems Manager Associati ons para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancia s administradas y le permite establecer líneas de referenci a de los niveles de parches del sistema operativo, las instalaci ones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6(1)	CM-6(1) Opciones de configura ción | Administr ación centraliz ada automatiz ada, aplicaciones y verificación	ec2- -comprobar managedinstance-pa tch-compliance-status	Habilite esta regla para ayudar a identific ar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimi entos de su organizac ión en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	mfa-enabled-for-iam-acceso desde la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.A	CM-6.A Opciones de configuración	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	mfa-enabled-for-iam-acceso desde la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.B	CM-6.B Opciones de configuración	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	mfa-enabled-for-iam-acceso desde la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.C	CM-6.C Opciones de configuración	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	mfa-enabled-for-iam-acceso desde la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-6.D	CM-6.D Opciones de configuración	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-7.A	CM-7.A Funcionalidad mínima	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-7.A	CM-7.A Funcionalidad mínima	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-7.B	CM-7.B Funcionalidad mínima	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-7.B	CM-7.B Funcionalidad mínima	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8(1)	CM-8(1) Inventario de componentes del sistema de informaci ón | Actualizaciones durante las instalaci ones y las retiradas	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8(1)	CM-8(1) Inventario de componentes del sistema de información | Actualizaciones durante las instalaciones y las retiradas	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8(2)	CM-8(2) Inventario de componentes del sistema de informaci ón | Mantenimiento automatizado	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8(2)	CM-8(2) Inventario de componentes del sistema de información | Mantenimiento automatizado	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventario de componentes del sistema de información | Detección automática de componentes no autorizados	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventario de componentes del sistema de información | Detección automática de componentes no autorizados	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventario de componentes del sistema de información | Detección automática de componentes no autorizados	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventario de componentes del sistema de información | Detección automática de componentes no autorizados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.A	CM-8.A Inventario de componentes del sistema de informaci ón	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.A	CM-8.A Inventario de componentes del sistema de información	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.B	CM-8.B Inventario de componentes del sistema de informaci ón	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.B	CM-8.B Inventario de componentes del sistema de información	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.C	CM-8.C Inventario de componentes del sistema de información	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.C	CM-8.C Inventario de componentes del sistema de información	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.D	CM-8.D Inventario de componentes del sistema de informaci ón	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.D	CM-8.D Inventario de componentes del sistema de información	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.E	CM-8.E Inventario de componentes del sistema de informaci ón	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CM-8.E	CM-8.E Inventario de componentes del sistema de información	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	elb-cross-zone-load-habilitado para el balanceo	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(5)	CP-2(5) Plan de contingencia | Continuar con las misiones y funciones empresariales esenciales	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(6)	CP-2(6) Plan de contingencia | Sitio alternativo de procesamiento o almacenamiento	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(6)	CP-2(6) Plan de contingencia | Sitio alternativo de procesamiento o almacenamiento	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(6)	CP-2(6) Plan de contingencia | Sitio alternativo de procesamiento o almacenamiento	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(6)	CP-2(6) Plan de contingencia | Sitio alternativo de procesamiento o almacenamiento	rds-cluster-multi-az-activado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(6)	CP-2(6) Plan de contingencia | Sitio alternativo de procesamiento o almacenamiento	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2(6)	CP-2(6) Plan de contingencia | Sitio alternativo de procesamiento o almacenamiento	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.A	CP-2.A Plan de contingencia	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.A	CP-2.A Plan de contingencia	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.A	CP-2.A Plan de contingencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CCCS-fPBMM-CP-2.A	CP-2.A Plan de contingencia	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.A	CP-2.A Plan de contingencia	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.A	CP-2.A Plan de contingencia	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.A	CP-2.A Plan de contingencia	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.A	CP-2.A Plan de contingencia	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.B	CP-2.B Plan de contingencia	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.B	CP-2.B Plan de contingencia	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.B	CP-2.B Plan de contingencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CCCS-fPBMM-CP-2.B	CP-2.B Plan de contingencia	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.B	CP-2.B Plan de contingencia	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.B	CP-2.B Plan de contingencia	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.B	CP-2.B Plan de contingencia	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.B	CP-2.B Plan de contingencia	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.C	CP-2.C Plan de contingencia	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.C	CP-2.C Plan de contingencia	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.C	CP-2.C Plan de contingencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CCCS-fPBMM-CP-2.C	CP-2.C Plan de contingencia	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.C	CP-2.C Plan de contingencia	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.C	CP-2.C Plan de contingencia	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.C	CP-2.C Plan de contingencia	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.C	CP-2.C Plan de contingencia	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.D	CP-2.D Plan de contingencia	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.D	CP-2.D Plan de contingencia	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.D	CP-2.D Plan de contingencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CCCS-fPBMM-CP-2.D	CP-2.D Plan de contingencia	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.D	CP-2.D Plan de contingencia	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.D	CP-2.D Plan de contingencia	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.D	CP-2.D Plan de contingencia	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.D	CP-2.D Plan de contingencia	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.E	CP-2.E Plan de contingencia	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.E	CP-2.E Plan de contingencia	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.E	CP-2.E Plan de contingencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CCCS-fPBMM-CP-2.E	CP-2.E Plan de contingencia	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.E	CP-2.E Plan de contingencia	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.E	CP-2.E Plan de contingencia	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.E	CP-2.E Plan de contingencia	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.E	CP-2.E Plan de contingencia	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.F	CP-2.F Plan de contingencia	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.F	CP-2.F Plan de contingencia	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.F	CP-2.F Plan de contingencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CCCS-fPBMM-CP-2.F	CP-2.F Plan de contingencia	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.F	CP-2.F Plan de contingencia	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.F	CP-2.F Plan de contingencia	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.F	CP-2.F Plan de contingencia	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.F	CP-2.F Plan de contingencia	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.G	CP-2.G Plan de contingencia	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.G	CP-2.G Plan de contingencia	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.G	CP-2.G Plan de contingencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CCCS-fPBMM-CP-2.G	CP-2.G Plan de contingencia	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.G	CP-2.G Plan de contingencia	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.G	CP-2.G Plan de contingencia	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.G	CP-2.G Plan de contingencia	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-2.G	CP-2.G Plan de contingencia	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(1)	CP-6(1) Sitio de almacenamiento alternativo | Separación del sitio principal	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6(2)	CP-6(2) Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.A	CP-6.A Sitio de almacenamiento alternativo	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-6.B	CP-6.B Sitio de almacenamiento alternativo	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(3)	CP-9(3) Copia de seguridad del sistema de información | Almacenamiento separado para información esencial	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(7)	CP-9(7) Copia de seguridad del sistema de información | Autorización doble	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9(7)	CP-9(7) Copia de seguridad del sistema de información | Autorización doble	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.A	CP-9.A Copia de seguridad del sistema de información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.AA	CP-9.AA Copia de seguridad del sistema de información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.B	CP-9.B Copia de seguridad del sistema de información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.C	CP-9.C Copia de seguridad del sistema de información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-9.D	CP-9.D Copia de seguridad del sistema de información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	elb-cross-zone-load-habilitado para el balanceo	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-CP-10.A	CP-10.A Recuperación y reconstitución del sistema de información	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(1)	IA-2(1) Identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas con privilegios	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(1)	IA-2(1) Identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas con privilegios	mfa-enabled-for-iam-acceso desde una consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(1)	IA-2(1) Identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas con privilegios	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(3)	IA-2(3) Identificación y autenticación (usuarios de la organización) | Acceso local a cuentas con privilegios	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(3)	IA-2(3) Identificación y autenticación (usuarios de la organización) | Acceso local a cuentas con privilegios	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(3)	IA-2(3) Identificación y autenticación (usuarios de la organización) | Acceso local a cuentas con privilegios	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(8)	IA-2(8) Identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas con privilegios - Resistente a la reproducción	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(8)	IA-2(8) Identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas con privilegios - Resistente a la reproducción	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(8)	IA-2(8) Identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas con privilegios - Resistente a la reproducción	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(11)	IA-2(11) Identificación y autenticación (usuarios de la organización) | Acceso remoto - Dispositivo independiente	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(11)	IA-2(11) Identificación y autenticación (usuarios de la organización) | Acceso remoto - Dispositivo independiente	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2(11)	IA-2(11) Identificación y autenticación (usuarios de la organización) | Acceso remoto - Dispositivo independiente	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2.A	IA-2.A Identificación y autenticación (usuarios de la organización)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2.A	IA-2.A Identificación y autenticación (usuarios de la organización)	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2.A	IA-2.A Identificación y autenticación (usuarios de la organización)	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-2.A	IA-2.A Identificación y autenticación (usuarios de la organización)	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4(4)	IA-4(4) Administración de identificadores | Identificar el estado del usuario	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.A	IA-4.A Administración de identificadores	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.A	IA-4.A Administración de identificadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.A	IA-4.A Administración de identificadores	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.B	IA-4.B Administración de identificadores	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.B	IA-4.B Administración de identificadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.B	IA-4.B Administración de identificadores	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.C	IA-4.C Administración de identificadores	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.C	IA-4.C Administración de identificadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.C	IA-4.C Administración de identificadores	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.D	IA-4.D Administración de identificadores	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.D	IA-4.D Administración de identificadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.D	IA-4.D Administración de identificadores	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.E	IA-4.E Administración de identificadores	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.E	IA-4.E Administración de identificadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-4.E	IA-4.E Administración de identificadores	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5(1)	IA-5(1) Administración de autenticadores | Autenticación basada en contraseñas	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5(2)	IA-5(2) Administración de autenticadores | Autenticación basada en PKI	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5(2)	IA-5(2) Administración de autenticadores | Autenticación basada en PKI	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5(4)	IA-5(4) Administración de autenticadores | Compatibilidad automatizada con la determinación de la seguridad de las contraseñas	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5(8)	IA-5(8) Administración de autenticadores | Cuentas de múltiples sistemas de informaci ón	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5(8)	IA-5(8) Administración de autenticadores | Cuentas de múltiples sistemas de informaci ón	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5(8)	IA-5(8) Administración de autenticadores | Cuentas de múltiples sistemas de información	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.A	IA-5.A Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.A	IA-5.A Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.A	IA-5.A Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.A	IA-5.A Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.B	IA-5.B Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.B	IA-5.B Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.B	IA-5.B Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.B	IA-5.B Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.C	IA-5.C Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.C	IA-5.C Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.C	IA-5.C Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.C	IA-5.C Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.D	IA-5.D Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.D	IA-5.D Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.D	IA-5.D Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.D	IA-5.D Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.E	IA-5.E Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.E	IA-5.E Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.E	IA-5.E Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.E	IA-5.E Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.F	IA-5.F Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.F	IA-5.F Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.F	IA-5.F Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.F	IA-5.F Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.G	IA-5.G Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.G	IA-5.G Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.G	IA-5.G Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.G	IA-5.G Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.H	IA-5.H Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.H	IA-5.H Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.H	IA-5.H Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.H	IA-5.H Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.I	IA-5.I Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.I	IA-5.I Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.I	IA-5.I Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.I	IA-5.I Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.J	IA-5.J Administración de autenticadores	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.J	IA-5.J Administración de autenticadores	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.J	IA-5.J Administración de autenticadores	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IA-5.J	IA-5.J Administración de autenticadores	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-IR-6(1)	IR-6(1) Informes de incidentes | Informes automatizados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-3.A	MA-3.A Herramientas de mantenimiento	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-3.A	MA-3.A Herramientas de mantenimiento	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MA-4(1)	MA-4(1) Mantenimiento no local | Auditoría y revisión	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-MP-2.A	MP-2.A Acceso multimedia	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-RA-5.A	RA-5.A Escaneo de vulnerabilidades	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-RA-5.B	RA-5.B Escaneo de vulnerabilidades	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-RA-5.C	RA-5.C Escaneo de vulnerabilidades	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-RA-5.D	RA-5.D Escaneo de vulnerabilidades	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-RA-5.E	RA-5.E Escaneo de vulnerabilidades	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SA-10(1)	SA-10(1) Administración de la configuración para desarrolladores | Verificación de la integridad del software y el firmware	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-5.A	SC-5.A Protección contra denegación de servicio	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-5.A	SC-5.A Protección contra denegación de servicio	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilidad de los recursos	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilidad de los recursos	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilidad de los recursos	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilidad de los recursos	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilidad de los recursos	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilidad de los recursos	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilidad de los recursos	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilidad de los recursos	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(3)	SC-7(3) Protección perimetral | Puntos de acceso	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomunicaciones externos	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomunicaciones externos	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomunicaciones externos	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomunicaciones externos	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	s3- bucket-level-publi c-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomunicaciones externos	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomunicaciones externos	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomunicaciones externos	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(4)	SC-7(4) Protección perimetral | Servicios de telecomun icaciones externos	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(5)	SC-7(5) Protección perimetral | Denegar de forma predeterm inada y permitir de forma excepcional	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(5)	SC-7(5) Protección perimetral | Denegar de forma predeterminada y permitir de forma excepcional	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(5)	SC-7(5) Protección perimetral | Denegar de forma predeterm inada y permitir de forma excepcional	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(5)	SC-7(5) Protección perimetral | Denegar de forma predeterminada y permitir de forma excepcional	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7(7)	SC-7(7) Protección perimetral | Evitar la tunelización dividida en dispositivos remotos	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.A	SC-7.A Protección perimetral	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.B	SC-7.B Protección perimetral	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-7.C	SC-7.C Protección perimetral	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8(1)	SC-8(1) Confidencialidad e integridad de la transmisión | Protección criptográfica o física alternativa	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-8(1)	SC-8(1) Confidencialidad e integridad de la transmisión | Protección criptográfica o física alternativa	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8(1)	SC-8(1) Confidencialidad e integridad de la transmisión | Protección criptográfica o física alternativa	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8(1)	SC-8(1) Confidencialidad e integridad de la transmisión | Protección criptográfica o física alternativa	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8(1)	SC-8(1) Confidencialidad e integridad de la transmisión | Protección criptográfica o física alternativa	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-SC-8(1)	SC-8(1) Confidencialidad e integridad de la transmisión | Protección criptográfica o física alternativa	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8(1)	SC-8(1) Confidencialidad e integridad de la transmisión | Protección criptográfica o física alternativa	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-8(1)	SC-8(1) Confidencialidad e integridad de la transmisión | Protección criptográfica o física alternativa	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8(1)	SC-8(1) Confidencialidad e integridad de la transmisión | Protección criptográfica o física alternativa	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-8.A	SC-8.A Confidencialidad e integridad de la transmisión	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8.A	SC-8.A Confidencialidad e integridad de la transmisión	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
CCCS-fPBMM-SC-8.A	SC-8.A Confidencialidad e integridad de la transmisión	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8.A	SC-8.A Confidencialidad e integridad de la transmisión	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8.A	SC-8.A Confidencialidad e integridad de la transmisión	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-SC-8.A	SC-8.A Confidencialidad e integridad de la transmisión	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8.A	SC-8.A Confidencialidad e integridad de la transmisión	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-8.A	SC-8.A Confidencialidad e integridad de la transmisión	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-8.A	SC-8.A Confidencialidad e integridad de la transmisión	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-12(1)	SC-12(1) Establecimiento y administración de claves criptográficas | Disponibilidad	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
CCCS-fPBMM-SC-12(2)	SC-12(2) Establecimiento y administración de claves criptográficas | Claves simétricas	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-12(2)	SC-12(2) Establecimiento y administración de claves criptográficas | Claves simétricas	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
CCCS-fPBMM-SC-12.A	SC-12.A Establecimiento y administración de claves criptográficas	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-12.A	SC-12.A Establecimiento y administración de claves criptográficas	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-201 7-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-13.A	SC-13.A Protección criptográfica	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-22.A	SC-22.A Arquitectura y aprovisionamiento para el servicio de resolución de nombres y direcciones	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CCCS-fPBMM-SC-23.A	SC-23.A Autenticidad de las sesiones	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-23.A	SC-23.A Autenticidad de las sesiones	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
CCCS-fPBMM-SC-23.A	SC-23.A Autenticidad de las sesiones	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-23.A	SC-23.A Autenticidad de las sesiones	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-23.A	SC-23.A Autenticidad de las sesiones	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-SC-23.A	SC-23.A Autenticidad de las sesiones	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-23.A	SC-23.A Autenticidad de las sesiones	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-23.A	SC-23.A Autenticidad de las sesiones	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-23.A	SC-23.A Autenticidad de las sesiones	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28(1)	SC-28(1) Protección de la información en reposo | Protección criptográfica	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SC-28.A	SC-28.A Protección de la información en reposo	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(2)	SI-2(2) Corrección de defectos | Estado automatizado de la corrección de defectos	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2(3)	SI-2(3) Corrección de defectos | Esfuerzo de corregir los defectos / Parámetros de referencia para las acciones correctivas	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.A	SI-2.A Corrección de defectos	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.B	SI-2.B Corrección de defectos	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.C	SI-2.C Corrección de defectos	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-2.D	SI-2.D Corrección de defectos	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3(1)	SI-3(1) Protección contra códigos maliciosos | Administración central	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3(7)	SI-3(7) Protecció n contra códigos maliciosos | Detección no basada en firmas	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.A	SI-3.A Protección contra códigos maliciosos	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.A	SI-3.A Protección contra códigos maliciosos	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.A	SI-3.A Protección contra códigos maliciosos	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.A	SI-3.A Protección contra códigos maliciosos	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.A	SI-3.A Protección contra códigos maliciosos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.B	SI-3.B Protección contra códigos maliciosos	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.B	SI-3.B Protección contra códigos maliciosos	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.B	SI-3.B Protección contra códigos maliciosos	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.B	SI-3.B Protección contra códigos maliciosos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.C	SI-3.C Protección contra códigos maliciosos	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.C	SI-3.C Protección contra códigos maliciosos	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.C	SI-3.C Protección contra códigos maliciosos	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.C	SI-3.C Protección contra códigos maliciosos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.D	SI-3.D Protección contra códigos maliciosos	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.D	SI-3.D Protección contra códigos maliciosos	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.D	SI-3.D Protección contra códigos maliciosos	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-3.D	SI-3.D Protección contra códigos maliciosos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(1)	SI-4(1) Monitoreo del sistema de informaci ón | Sistema de detección de intrusos en todo el sistema	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(1)	SI-4(1) Monitoreo del sistema de informaci ón | Sistema de detección de intrusos en todo el sistema	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(2)	SI-4(2) Monitoreo del sistema de informaci ón | Herramientas automatizadas para análisis en tiempo real	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(2)	SI-4(2) Monitoreo del sistema de informaci ón | Herramientas automatizadas para análisis en tiempo real	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(4)	SI-4(4) Monitoreo del sistema de información | Tráfico de comunicaciones entrantes y salientes	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(4)	SI-4(4) Monitoreo del sistema de información | Tráfico de comunicaciones entrantes y salientes	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(5)	SI-4(5) Monitoreo del sistema de información | Alertas generadas por el sistema	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(11)	SI-4(11) Monitoreo del sistema de informaci ón | Análisis de las anomalías del tráfico de comunicaciones	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(11)	SI-4(11) Monitoreo del sistema de informaci ón | Análisis de las anomalías del tráfico de comunicaciones	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(16)	SI-4(16) Monitoreo del sistema de informaci ón | Correlacionar la información de monitoreo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(16)	SI-4(16) Monitoreo del sistema de informaci ón | Correlacionar la información de monitoreo	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(20)	SI-4(20) Monitoreo del sistema de información | Usuario con privilegios	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(23)	SI-4(23) Monitoreo del sistema de informaci ón | Dispositivos basados en el host	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4(23)	SI-4(23) Monitoreo del sistema de informaci ón | Dispositivos basados en el host	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.A	SI-4.A Monitoreo del sistema de información	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.A	SI-4.A Monitoreo del sistema de informaci ón	cloud-trail-log-file-validación habilitada	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.A	SI-4.A Monitoreo del sistema de informaci ón	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CCCS-fPBMM-SI-4.A	SI-4.A Monitoreo del sistema de informaci ón	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.A	SI-4.A Monitoreo del sistema de informaci ón	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.B	SI-4.B Monitoreo del sistema de información	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.B	SI-4.B Monitoreo del sistema de informaci ón	cloud-trail-log-file-validación habilitada	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.B	SI-4.B Monitoreo del sistema de informaci ón	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CCCS-fPBMM-SI-4.B	SI-4.B Monitoreo del sistema de informaci ón	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.B	SI-4.B Monitoreo del sistema de informaci ón	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.C	SI-4.C Monitoreo del sistema de información	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.C	SI-4.C Monitoreo del sistema de informaci ón	cloud-trail-log-file-validación habilitada	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.C	SI-4.C Monitoreo del sistema de informaci ón	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CCCS-fPBMM-SI-4.C	SI-4.C Monitoreo del sistema de informaci ón	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.C	SI-4.C Monitoreo del sistema de informaci ón	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.D	SI-4.D Monitoreo del sistema de información	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.D	SI-4.D Monitoreo del sistema de informaci ón	cloud-trail-log-file-validación habilitada	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.D	SI-4.D Monitoreo del sistema de informaci ón	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CCCS-fPBMM-SI-4.D	SI-4.D Monitoreo del sistema de informaci ón	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.D	SI-4.D Monitoreo del sistema de informaci ón	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.E	SI-4.E Monitoreo del sistema de información	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.E	SI-4.E Monitoreo del sistema de informaci ón	cloud-trail-log-file-validación habilitada	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.E	SI-4.E Monitoreo del sistema de informaci ón	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CCCS-fPBMM-SI-4.E	SI-4.E Monitoreo del sistema de informaci ón	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.E	SI-4.E Monitoreo del sistema de informaci ón	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.F	SI-4.F Monitoreo del sistema de información	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.F	SI-4.F Monitoreo del sistema de informaci ón	cloud-trail-log-file-validación habilitada	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.F	SI-4.F Monitoreo del sistema de informaci ón	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CCCS-fPBMM-SI-4.F	SI-4.F Monitoreo del sistema de informaci ón	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.F	SI-4.F Monitoreo del sistema de informaci ón	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.G	SI-4.G Monitoreo del sistema de informaci ón	cloudwatch-alarm-a ction-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluació n. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.G	SI-4.G Monitoreo del sistema de informaci ón	cloud-trail-log-file-validación habilitada	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.G	SI-4.G Monitoreo del sistema de informaci ón	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CCCS-fPBMM-SI-4.G	SI-4.G Monitoreo del sistema de informaci ón	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-4.G	SI-4.G Monitoreo del sistema de informaci ón	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-5.A	SI-5.A Alertas, avisos y directivas de seguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-5.B	SI-5.B Alertas, avisos y directivas de seguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-5.C	SI-5.C Alertas, avisos y directivas de seguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-5.D	SI-5.D Alertas, avisos y directivas de seguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-7(1)	SI-7(1) Integridad del software, el firmware y la información | Controles de integrida d	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-7(7)	SI-7(7) Integridad del software, el firmware y la información | Integración de la detección y la respuesta	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-7.A	SI-7.A Integridad del software, el firmware y la información	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CCCS-fPBMM-SI-12.A	SI-12.A Gestión y retención de información	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

Plantilla

La plantilla está disponible en GitHub: Perfil de control de nubes medianas del Centro Canadiense de Ciberseguridad (CCCS) sobre las mejores prácticas operativas.

Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4 Level 1

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costos mediante reglas administradas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre Amazon Web Services Foundation v1.4 Level 1 del Center for Internet Security (CIS) y las reglas de AWS Config configuración/comprobaciones de procesos AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de nivel 1 de Amazon Web Services Foundation v1.4 de CIS. Un control de Amazon Web Services Foundation v1.4 Level 1 del CIS puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Para obtener más información sobre las verificaciones de procesos, consulte process-checks.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Mantener los datos de contacto actuales	account-contact-details-configured (verificación del proceso)	Asegúrese de que el correo electrónico y el número de teléfono de contacto de las cuentas de AWS estén actualizados y correspondan a más de una persona de su organización. En la sección Mi cuenta de la consola, asegúrese de que se especifiq ue la informaci ón correcta en la sección Informaci ón de contacto. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/
1.2	Garantizar que se registre la información de contacto de seguridad	account-security-contact-configured (Verificación del proceso)	Compruebe que el correo electrónico y el número de teléfono de contacto del equipo de seguridad de la organización estén actualizados. En la sección Mi cuenta de la consola de AWS administración, asegúrese de que se especifique la información correcta en la sección de seguridad. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4	Garantizar que no exista ninguna clave de acceso de usuario raíz	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5	Garantizar que la MFA esté habilitada para el usuario raíz	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.7	Eliminar el uso del usuario raíz para las tareas administrativas y diarias	root-account-regular-use (Verificación del proceso)	Compruebe que se evite usar la cuenta raíz para las tareas diarias. En IAM, ejecute un informe de credenciales para examinar cuándo se utilizó el usuario raíz por última vez. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.8	Garantizar que la política de contraseñ as de IAM requiera una longitud mínima de 14 o más	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.9	Garantizar que la política de contraseñ as de IAM impida la reutilización de contraseñas	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.10	Garantizar que la autenticación multifactor (MFA) esté habilitada para todos los usuarios que tengan una contraseña para la consola	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.11	No configurar claves de acceso durante la configuración de usuario inicial para todos los usuarios que tienen una contraseña para la consola	iam-user-console-and- api-access-at-creation (Verificación del proceso)	Asegúrese de que no se hayan configurado claves de acceso durante la configuración de usuario inicial para todos los usuarios que tienen una contraseña para la consola. Para todos los usuarios con acceso a la consola, compare la hora de creación del usuario con la fecha de creación de la clave de acceso. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.12	Garantizar que se deshabiliten las credenciales no usadas durante 45 días o más	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor para la maxCredentialUsage Edad (valor estándar de la CEI: 45). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.13	Garantizar que solo haya una clave de acceso activa disponible para cada usuario	iam-user-single-access-key (verificación del proceso)	Garantice que solo haya una clave de acceso activa disponible para cada usuario. Para todos los usuarios, debe comprobar que solo se utilice una clave activa en la pestaña Credenciales de seguridad para cada usuario en IAM. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.14	Garantizar que las claves de acceso se roten cada 90 días o menos	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.15	Garantizar que los usuarios reciban permisos solo a través de grupos	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.15	Garantizar que los usuarios reciban permisos solo a través de grupos	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.15	Garantizar que los usuarios reciban permisos solo a través de grupos	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.16	Asegurar que no se adjunten políticas de IAM que permitan privilegios administrativos completos “*:*”	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1,17	Asegúrese de que se haya creado un rol de soporte para gestionar los incidente s con AWS Support	iam-policy-in-use	AWS Identity and Access Management (IAM) puede ayudarle a gestionar los permisos y autorizac iones de acceso al garantizar que las políticas de IAM se asignen a los usuarios, roles o grupos adecuados. La restricción de estas políticas también incorpora los principio s de privilegio mínimo y la separación de funciones. Esta regla requiere que defina PolicyArn en arn:aws:i am: AWSSuppor t :aws:policy/ Access, para la gestión de incidentes con Support. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.19	Asegúrese de eliminar todos los SSL/TLS certificados caducados almacenados en AWS IAM	iam-expired-certificates (Verificación del proceso)	Asegúrese de eliminar todos los SSL/TLS certificados caducados almacenados en IAM. Desde la línea de comandos con la AWS CLI instalada, ejecute el comando 'AWS iam list-server-certificates' y determine si hay algún certificado de servidor caducado. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.20	Asegúrese de que AWS IAM Access Analyzer esté activado	iam-access-analyzer-enabled (Verificación del proceso)	Garantizar que IAM Access Analyzer esté activado. En la sección de IAM de la consola, seleccione Access Analyzer y asegúrese de que el STATUS esté establecido en Activo. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1.3	Garantizar que la eliminación de la MFA esté habilitada en los buckets de S3	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Para añadir la eliminación de la autenticación multifactor (MFA) a un bucket de S3 se requiere un factor de autenticación adicional para cambiar el estado de la versión del bucket o para eliminar la versión del objeto. La eliminación de la MFA puede añadir una capa de seguridad adicional en caso de que las credenciales de seguridad se vean comprometidas o se conceda un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1.5	Garantizar que los buckets de S3 estén configurados con Bloquear acceso público (configuración del bucket)	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1.5	Garantizar que los buckets de S3 estén configurados con Bloquear acceso público (configuración del bucket)	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
2.2.1	Garantizar que el cifrado de volumen de EBS esté activado	encrypted-volumes	Como los datos confidenciales pueden existir y para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.1	Garantizar que el cifrado de volumen de EBS esté activado	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
2.3.1	Garantizar que el cifrado esté habilitado para las instancias de RDS	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.3.1	Garantizar que el cifrado esté habilitado para las instancias de RDS	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1	Asegúrese de que CloudTrail esté activado en todas las regiones	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Asegúrese de que el depósito de S3 utilizado para almacenar CloudTrail los registros no sea de acceso público	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
3.3	Asegúrese de que el depósito de S3 utilizado para almacenar CloudTrail los registros no sea de acceso público	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Asegúrese de que el depósito de S3 utilizado para almacenar CloudTrail los registros no sea de acceso público	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
3.4	Asegúrese de que CloudTrail las rutas estén integradas con los registros CloudWatch	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6	Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Garantizar que haya un filtro de métricas de registro y una alarma para las llamadas a la API no autorizadas	alarm-unauthorized-api-calls (Verificación del proceso)	Garantizar que haya un filtro de métricas de registro y una alarma para las llamadas a la API no autorizadas Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2	Garantizar que haya un filtro de métricas de registro y una alarma de registro para el inicio de sesión en la sin MFA en la consola de administración	alarm-sign-in-without-mfa (Comprobación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para el inicio de sesión en la Consola de administración de AWS sin autentica ción multifactor (MFA). Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.3	Garantizar que haya un filtro de métricas de registro y una alarma para el uso de la cuenta raíz	alarm-root-account-use (Verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para usar la cuenta raíz. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de IAM	alarm-iam-policy-change (Verificación del proceso)	Garantice que haya un filtro de métricas de registro y una alarma para los cambios de política de IAM. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.5	Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de configuración de CloudTrail	alarm-cloudtrail-config-change (Verificación del proceso)	Asegúrese de que haya un filtro de registro métrico y una alarma para los cambios AWS Cloud Trail de configuración. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de bucket de S3	alarm-s3- bucket-policy-change (Verificación del proceso)	Garantice que haya un filtro de métricas de registro y una alarma para los cambios de política de bucket de Amazon S3. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.12	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en las puertas de enlace de la red	alarm-vpc-network-gateway-change (verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en las puertas de enlace de la red. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.13	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la tabla de enrutamiento	alarm-vpc-route-table-change (verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en la tabla de enrutamiento. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.14	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la VPC	alarm-vpc-change (Verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en la Amazon Virtual Private Cloud (VPC). Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.15	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en AWS Organizations	alarm-organizations-change (Verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en AWS Organizations. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.1	Asegúrese de que ninguna red ACLs permita la entrada desde el 0.0.0.0/0 a los puertos de administración remota del servidor	nacl-no-unrestricted-ssh-rdp	Asegúrese de que ninguna red ACLs permita la entrada pública a los puertos de administración remota del servidor. En la sección de VPC de la consola, asegúrese de que haya una red ACLs con una fuente de «0.0.0.0/0» con puertos o rangos de puertos permitidos, incluidos los puertos de administración remota del servidor. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Garantizar que ningún grupo de seguridad permita la entrada desde 0.0.0.0/0 a los puertos de administr ación de servidores remotos	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Garantizar que ningún grupo de seguridad permita la entrada desde 0.0.0.0/0 a los puertos de administración de servidores remotos	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valor estándar del CIS: 3389). Los valores reales deben reflejar las políticas de su organización.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4 Level 1.

Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4 Level 2

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de control de seguridad, operativos o de optimización de costos mediante AWS Config reglas administradas o personalizadas y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el Centro de Seguridad de Internet (CIS) Amazon Web Services Foundation v1.4 Level 2 y las reglas de AWS Config configuración/comprobaciones de procesos AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de nivel 2 de Amazon Web Services Foundation v1.4 de CIS. Un control de Amazon Web Services Foundation v1.4 Level 2 del CIS puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Para obtener más información sobre las verificaciones de procesos, consulte process-checks.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Mantener los datos de contacto actuales	account-contact-details-configured (verificación del proceso)	Asegúrese de que el correo electrónico y el número de teléfono de contacto de las cuentas de AWS estén actualizados y correspondan a más de una persona de su organización. En la sección Mi cuenta de la consola, asegúrese de que se especifiq ue la informaci ón correcta en la

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			sección Informaci ón de contacto. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2	Garantizar que se registre la informaci ón de contacto de seguridad	account-security-c ontact-configured (Verificación del proceso)	Compruebe que el correo electrónico y el número de teléfono de contacto del equipo de seguridad de la organización estén actualizados. En la sección Mi cuenta de la consola de AWS administr ación, asegúrese de que se especifiq ue la informaci ón correcta en la sección de seguridad . Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity. org/benchmark/amaz on_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4	Garantizar que no exista ninguna clave de acceso de usuario raíz	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5	Garantizar que la MFA esté habilitada para el usuario raíz	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.6	Garantizar que la MFA basada en hardware esté activada para la cuenta de usuario raíz	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.7	Eliminar el uso del usuario raíz para las tareas administrativas y diarias	root-account-regular-use (Verificación del proceso)	Compruebe que se evite usar la cuenta raíz para las tareas diarias. En IAM, ejecute un informe de credenciales para examinar cuándo se utilizó el usuario raíz por última vez. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.8	Garantizar que la política de contraseñ as de IAM requiera una longitud mínima de 14 o más	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.9	Garantizar que la política de contraseñas de IAM impida la reutilización de contraseñas	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.10	Garantizar que la autenticación multifactor (MFA) esté habilitada para todos los usuarios que tengan una contraseña para la consola	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.11	No configurar claves de acceso durante la configuración de usuario inicial para todos los usuarios que tienen una contraseña para la consola	iam-user-console-and- api-access-at-creation (Verificación del proceso)	Asegúrese de que no se hayan configurado claves de acceso durante la configuración de usuario inicial para todos los usuarios que tienen una contraseña para la consola. Para todos los usuarios con acceso a la consola, compare la hora de creación del usuario con la fecha de creación de la clave de acceso. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.12	Garantizar que se deshabiliten las credenciales no usadas durante 45 días o más	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor para la maxCredentialUsage Edad (valor estándar de la CEI: 45). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.13	Garantizar que solo haya una clave de acceso activa disponible para cada usuario	iam-user-single-access-key (verificación del proceso)	Garantice que solo haya una clave de acceso activa disponible para cada usuario. Para todos los usuarios, debe comprobar que solo se utilice una clave activa en la pestaña Credenciales de seguridad para cada usuario en IAM. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.14	Garantizar que las claves de acceso se roten cada 90 días o menos	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.15	Garantizar que los usuarios reciban permisos solo a través de grupos	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.15	Garantizar que los usuarios reciban permisos solo a través de grupos	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.15	Garantizar que los usuarios reciban permisos solo a través de grupos	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.16	Asegurar que no se adjunten políticas de IAM que permitan privilegios administrativos completos “*:*”	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1,17	Asegúrese de que se haya creado un rol de soporte para gestionar los incidente s con AWS Support	iam-policy-in-use	AWS Identity and Access Management (IAM) puede ayudarle a gestionar los permisos y autorizac iones de acceso al garantizar que las políticas de IAM se asignen a los usuarios, roles o grupos adecuados. La restricción de estas políticas también incorpora los principio s de privilegio mínimo y la separación de funciones. Esta regla requiere que defina PolicyArn en arn:aws:i am: AWSSuppor t :aws:policy/ Access, para la gestión de incidentes con Support. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.18	Asegúrese de que las funciones de instancia de IAM se utilicen para acceder a los AWS recursos desde las instancias	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.19	Asegúrese de eliminar todos los SSL/TLS certificados caducados almacenados en AWS IAM	iam-expired-certificates (Verificación del proceso)	Asegúrese de eliminar todos los SSL/TLS certificados caducados almacenados en IAM. Desde la línea de comandos con la AWS CLI instalada, ejecute el comando 'AWS iam list-server-certificates' y determine si hay algún certificado de servidor caducado. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.20	Asegúrese de que AWS IAM Access Analyzer esté activado	iam-access-analyzer-enabled (Verificación del proceso)	Garantizar que IAM Access Analyzer esté activado. En la sección de IAM de la consola, seleccione Access Analyzer y asegúrese de que el STATUS esté establecido en Activo. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.21	Asegúrese de que los usuarios se gestionen de forma centralizada desde la federación de identidades o desde AWS Organizations para entornos con varias cuentas	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
2.1.1	Asegúrese de que todos los cubos de S3 utilicen encryption-at-rest	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1.2	Garantizar que la política de buckets de S3 esté configura da para denegar las solicitudes HTTP	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1.3	Garantizar que la eliminación de la MFA esté habilitada en los buckets de S3	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Para añadir la eliminación de la autenticación multifactor (MFA) a un bucket de S3 se requiere un factor de autenticación adicional para cambiar el estado de la versión del bucket o para eliminar la versión del objeto. La eliminación de la MFA puede añadir una capa de seguridad adicional en caso de que las credenciales de seguridad se vean comprometidas o se conceda un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1.5	Garantizar que los buckets de S3 estén configurados con Bloquear acceso público (configuración del bucket)	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1.5	Garantizar que los buckets de S3 estén configurados con Bloquear acceso público (configuración del bucket)	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
2.2.1	Garantizar que el cifrado de volumen de EBS esté activado	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.1	Garantizar que el cifrado de volumen de EBS esté activado	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
2.3.1	Garantizar que el cifrado esté habilitado para las instancias de RDS	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.3.1	Garantizar que el cifrado esté habilitado para las instancias de RDS	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1	Asegúrese de que CloudTrail esté activado en todas las regiones	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2	Asegúrese de que la validación del archivo de CloudTrail registro esté habilitada	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
3.3	Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
3.4	Asegúrese de que CloudTrail las rutas estén integradas con los registros CloudWatch	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5	Asegúrese de que AWS Config esté activado en todas las regiones	config-enabled-all-regions (Verificación del proceso)	Asegúrese de que AWS Config esté activado en todas AWS las regiones. En la sección AWS Config de la consola, para cada región habilitada, asegúrese de que la grabadora AWS Config esté configurada correctamente. Asegúrese de que el registro de los recursos globales de AWS esté habilitado al menos en una región. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6	Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de S3 CloudTrail	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7	Asegúrese de que CloudTrail los registros estén cifrados en reposo mediante KMS CMKs	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
3.8	Asegúrese de que la rotación para los clientes creados CMKs esté habilitada	cmk-backing-key-rotation-activado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.9	Asegúrese de que el registro de flujo de VPC esté habilitado en todos VPCs	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
3.10	Garantizar que el registro en el nivel de objeto para los eventos de escritura esté habilitado para el bucket de S3	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Garantizar que el registro en el nivel de objeto para los eventos de lectura esté habilitado para el bucket de S3	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
4.1	Garantizar que haya un filtro de métricas de registro y una alarma para las llamadas a la API no autorizadas	alarm-unauthorized-api-calls (Verificación del proceso)	Garantizar que haya un filtro de métricas de registro y una alarma para las llamadas a la API no autorizadas Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2	Garantizar que haya un filtro de métricas de registro y una alarma de registro para el inicio de sesión en la sin MFA en la consola de administración	alarm-sign-in-without-mfa (Comprobación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para el inicio de sesión en la Consola de administración de AWS sin autentica ción multifactor (MFA). Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.3	Garantizar que haya un filtro de métricas de registro y una alarma para el uso de la cuenta raíz	alarm-root-account-use (Verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para usar la cuenta raíz. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de IAM	alarm-iam-policy-change (Verificación del proceso)	Garantice que haya un filtro de métricas de registro y una alarma para los cambios de política de IAM. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.5	Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de configura ción de CloudTrail	alarm-cloudtrail-c onfig-change (Verifica ción del proceso)	Asegúrese de que haya un filtro de registro métrico y una alarma para los cambios AWS Cloud Trail de configura ción. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Garantizar que haya un filtro de métricas de registro y una alarma para los errores de autentica ción de la Consola de administración de AWS	alarm-console-auth-failures (Verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los errores de autentica ción de la Consola de administración de AWS . Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.7	Asegúrese de que existan un registro, un filtro métrico y una alarma para deshabilitar o eliminar de forma programada los datos creados por el cliente CMKs	alarm-kms-disable-or-delete-cmk (verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para deshabilitar o eliminar de forma programada los datos creados por el cliente. CMKs Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de bucket de S3	alarm-s3- bucket-policy-change (Verificación del proceso)	Garantice que haya un filtro de métricas de registro y una alarma para los cambios de política de bucket de Amazon S3. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.9	Asegúrese de que existan un filtro de métrica de registro y una alarma para los cambios de configura ción de AWS Config	alarm-aws-config-c hange (Verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios de configura ción de AWS Confi g. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity. org/benchmark/amaz on_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.10	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de grupos de seguridad	alarm-vpc-secrity-group-change (verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en los grupos de seguridad. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.11	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)	alarm-vpc-nacl-change (Verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL). Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.12	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en las puertas de enlace de la red	alarm-vpc-network-gateway-change (verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en las puertas de enlace de la red. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.13	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la tabla de enrutamiento	alarm-vpc-route-table-change (verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en la tabla de enrutamiento. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.14	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la VPC	alarm-vpc-change (Verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en la Amazon Virtual Private Cloud (VPC). Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.15	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en AWS Organizations	alarm-organizations-change (Verificación del proceso)	Asegúrese de que haya un filtro de métricas de registro y una alarma para los cambios en AWS Organizations. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.1	Asegúrese de que ninguna red ACLs permita la entrada desde el 0.0.0.0/0 a los puertos de administración remota del servidor	nacl-no-unrestricted-ssh-rdp	Asegúrese de que ninguna red ACLs permita la entrada pública a los puertos de administración remota del servidor. En la sección de VPC de la consola, asegúrese de que haya una red ACLs con una fuente de «0.0.0.0/0» con puertos o rangos de puertos permitidos, incluidos los puertos de administración remota del servidor. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Garantizar que ningún grupo de seguridad permita la entrada desde 0.0.0.0/0 a los puertos de administr ación de servidores remotos	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Garantizar que ningún grupo de seguridad permita la entrada desde 0.0.0.0/0 a los puertos de administración de servidores remotos	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valor estándar del CIS: 3389). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3	Garantizar que el grupo de seguridad predeterminado de cada VPC limite todo el tráfico	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4	Garantizar que las tablas de enrutamiento para el emparejamiento de VPC tengan “acceso mínimo”	vpc-peering-least-access (Verificación del proceso)	Asegúrese de que las tablas de enrutamiento para el emparejamiento de VPC tengan “acceso mínimo”. En la sección de VPC de la consola, examine las entradas de la tabla de enrutamiento para asegurarse de que se pueda enrutar el menor número de subredes o hosts necesarios para cumplir con el propósito del emparejamiento. Para obtener más información sobre la auditoría de este control, consulte el documento CIS Amazon Web Services Foundations Benchmark versión 1.4.0, disponible en https://www.cisecurity.org/benchmark/amazon_web_services/

Plantilla

La plantilla está disponible en GitHub: Best Practices Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2.

Mejores prácticas operativas para los controles de seguridad críticos de CIS v8 IG1

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los Controles de seguridad críticos de Center for Internet Security (CIS) v8 IG1 y las reglas de Config AWS administradas. Cada una AWS Config se aplica a un AWS recurso específico y se refiere a uno o más controles de CIS Critical Security Controls v8 IG1. Un IG1 control CIS Critical Security Controls v8 puede estar relacionado con varias AWS Config reglas. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec-2 security-group-attached-to -es	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Asegurarse de que el software autorizado o sea compatible actualmente	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Asegurarse de que el software autorizado sea compatible actualmente	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Asegurarse de que el software autorizado sea compatible actualmente	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.
3.3	Configurar listas de control de acceso a datos	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.3	Configurar listas de control de acceso a datos	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
3.3	Configurar listas de control de acceso a datos	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.3	Configurar listas de control de acceso a datos	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
3.3	Configurar listas de control de acceso a datos	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
3.3	Configurar listas de control de acceso a datos	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.3	Configurar listas de control de acceso a datos	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.3	Configurar listas de control de acceso a datos	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
3.3	Configurar listas de control de acceso a datos	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.
3.3	Configurar listas de control de acceso a datos	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegi o mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).
3.3	Configurar listas de control de acceso a datos	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	efs-access-point-enforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.
3.4	Hacer cumplir la retención de datos	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Hacer cumplir la retención de datos	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
4.1	Establecer y mantener un proceso de configuración seguro	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	efs-access-point-enforce-directorio-raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.
4.1	Establecer y mantener un proceso de configuración seguro	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Administrar el software y los activos empresariales de forma segura	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
4.6	Administrar el software y los activos empresariales de forma segura	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Administrar el software y los activos empresariales de forma segura	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
4.6	Administrar el software y los activos empresariales de forma segura	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Administrar el software y los activos empresariales de forma segura	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
4.6	Administrar el software y los activos empresariales de forma segura	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.7	Administrar las cuentas predeterminadas del software y los activos empresariales	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.1	Establecer y mantener un inventario de las cuentas	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3	Deshabilitar las cuentas inactivas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4	Restringir los privilegios de administrador a las cuentas de administrador dedicadas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4	Restringir los privilegios de administrador a las cuentas de administrador dedicadas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4	Requerir la MFA para el acceso remoto a la red	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4	Requerir la MFA para el acceso remoto a la red	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4	Requerir la MFA para el acceso remoto a la red	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.5	Requerir la MFA para el acceso administrativo	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1	Establecer y mantener un proceso de administración de vulnerabilidades	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1	Establecer y mantener un proceso de administración de vulnerabilidades	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1	Establecer y mantener un proceso de administración de vulnerabilidades	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
7.3	Administrar los parches del sistema operativo de forma automática	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3	Administrar los parches del sistema operativo de forma automática	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3	Administrar los parches del sistema operativo de forma automática	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.4	Administrar los parches de las aplicaciones de forma automática	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.4	Administrar los parches de las aplicaciones de forma automática	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.4	Administrar los parches de las aplicaciones de forma automática	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Establecer y mantener un proceso de administración de registros de auditoría	audit-log-policy-exists (Verificación del proceso)	Establezca y mantenga una política de administración de registros de auditoría que defina los requisitos de registro de su organización. Esto incluye, pero no se limita a, la revisión y la conservación de los registros de auditoría.
8.2	Recopilar los registros de auditoría	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
8.2	Recopilar los registros de auditoría	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3	Garantizar el almacenamiento adecuado de los registros de auditoría	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implementar y mantener un software antimalware	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2	Configurar las actualizaciones automáticas de firmas antimalware	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	ebs-optimized-inst ance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operation s. This optimization provides the most efficient performan ce for your EBS volumes by minimizin g contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automáticas	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	redshift-cluster-m aintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configura ción preferida para su organización. En concreto, que tengan períodos de mantenimi ento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVers ionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).
11.3	Proteger los datos de recuperación	backup-recovery-po int-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Proteger los datos de recuperación	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
11.3	Proteger los datos de recuperación	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Proteger los datos de recuperación	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para los controles de seguridad críticos del CIS v8 IG1.

Mejores prácticas operativas para los controles de seguridad críticos de CIS v8 IG2

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los Controles de seguridad críticos de Center for Internet Security (CIS) v8 IG2 y las reglas de Config AWS administradas. Cada una AWS Config se aplica a un AWS recurso específico y se refiere a uno o más controles de CIS Critical Security Controls v8 IG2. Un IG2 control CIS Critical Security Controls v8 puede estar relacionado con varias AWS Config reglas. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			durante más días de los permitidos, de acuerdo con los estándares de su organización.
1.1	Establecer y mantener un inventario detallado de los activos empresariales	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec-2 security-group-attached-to -es	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Asegurarse de que el software autorizado o sea compatible actualmente	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Asegurarse de que el software autorizado sea compatible actualmente	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Asegurarse de que el software autorizado sea compatible actualmente	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.4	Utilizar herramientas automatizadas de inventario de software	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.4	Utilizar herramientas automatizadas de inventario de software	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.
3.3	Configurar listas de control de acceso a datos	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.3	Configurar listas de control de acceso a datos	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
3.3	Configurar listas de control de acceso a datos	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.3	Configurar listas de control de acceso a datos	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
3.3	Configurar listas de control de acceso a datos	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
3.3	Configurar listas de control de acceso a datos	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.3	Configurar listas de control de acceso a datos	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.3	Configurar listas de control de acceso a datos	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
3.3	Configurar listas de control de acceso a datos	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
3.3	Configurar listas de control de acceso a datos	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegi o mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).
3.3	Configurar listas de control de acceso a datos	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	efs-access-point-enforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.
3.4	Hacer cumplir la retención de datos	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Hacer cumplir la retención de datos	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.
3.10	Cifrar los datos confidenciales en tránsito	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.10	Cifrar los datos confidenciales en tránsito	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.10	Cifrar los datos confidenciales en tránsito	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.10	Cifrar los datos confidenciales en tránsito	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
3.10	Cifrar los datos confidenciales en tránsito	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.11	Cifrar los datos confidenciales en reposo	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
3.11	Cifrar los datos confidenciales en reposo	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
3.11	Cifrar los datos confidenciales en reposo	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
3.11	Cifrar los datos confidenciales en reposo	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.
3.11	Cifrar los datos confidenciales en reposo	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
3.11	Cifrar los datos confidenciales en reposo	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
3.11	Cifrar los datos confidenciales en reposo	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
4.1	Establecer y mantener un proceso de configuración seguro	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	efs-access-point-enforce-directorio-raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.
4.1	Establecer y mantener un proceso de configuración seguro	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Administrar el software y los activos empresariales de forma segura	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
4.6	Administrar el software y los activos empresariales de forma segura	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Administrar el software y los activos empresariales de forma segura	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
4.6	Administrar el software y los activos empresariales de forma segura	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Administrar el software y los activos empresariales de forma segura	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
4.6	Administrar el software y los activos empresariales de forma segura	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.7	Administrar las cuentas predeterminadas del software y los activos empresariales	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.1	Establecer y mantener un inventario de las cuentas	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3	Deshabilitar las cuentas inactivas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4	Restringir los privilegios de administrador a las cuentas de administrador dedicadas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4	Restringir los privilegios de administrador a las cuentas de administrador dedicadas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.6	Centralizar la administración de cuentas	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4	Requerir la MFA para el acceso remoto a la red	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4	Requerir la MFA para el acceso remoto a la red	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4	Requerir la MFA para el acceso remoto a la red	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.5	Requerir la MFA para el acceso administrativo	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.7	Centralizar el control de los accesos	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1	Establecer y mantener un proceso de administración de vulnerabilidades	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1	Establecer y mantener un proceso de administración de vulnerabilidades	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1	Establecer y mantener un proceso de administración de vulnerabilidades	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
7.3	Administrar los parches del sistema operativo de forma automática	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3	Administrar los parches del sistema operativo de forma automática	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3	Administrar los parches del sistema operativo de forma automática	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.4	Administrar los parches de las aplicaciones de forma automática	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.4	Administrar los parches de las aplicaciones de forma automática	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.4	Administrar los parches de las aplicaciones de forma automática	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.5	Realizar los escaneos automatizados de vulnerabilidades de los activos internos de la empresa	ecr-private-image-scanning-activado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identific ar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.
8.1	Establecer y mantener un proceso de administración de registros de auditoría	audit-log-policy-e xists (Verificación del proceso)	Establezca y mantenga una política de administr ación de registros de auditoría que defina los requisito s de registro de su organización. Esto incluye, pero no se limita a, la revisión y la conservación de los registros de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
8.2	Recopilar los registros de auditoría	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3	Garantizar el almacenamiento adecuado de los registros de auditoría	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).
8.5	Recopilar registros de auditoría detallados	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
8.5	Recopilar registros de auditoría detallados	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.7	Recopilar registros de auditoría de solicitud es de URL	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.9	Centralizar los registros de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
8.10	Conservar los registros de auditoría	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.10	Conservar los registros de auditoría	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implementar y mantener un software antimalware	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2	Configurar las actualizaciones automáticas de firmas antimalware	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4	Configurar el escaneo antimalwa re automático de los medios extraíbles	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6	Administrar el software antimalware de forma centralizada	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7	Utilizar un software antimalware basado en el comportamiento	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	ebs-optimized-inst ance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operation s. This optimization provides the most efficient performan ce for your EBS volumes by minimizin g contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automáticas	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	redshift-cluster-m aintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configura ción preferida para su organización. En concreto, que tengan períodos de mantenimi ento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVers ionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).
11.3	Proteger los datos de recuperación	backup-recovery-po int-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Proteger los datos de recuperación	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
11.3	Proteger los datos de recuperación	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Proteger los datos de recuperación	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
12.2	Establecer y mantener una arquitectura de red segura	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
12.2	Establecer y mantener una arquitectura de red segura	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS
12.2	Establecer y mantener una arquitectura de red segura	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
12.2	Establecer y mantener una arquitectura de red segura	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
12.2	Establecer y mantener una arquitectura de red segura	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
12.2	Establecer y mantener una arquitectura de red segura	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
12.2	Establecer y mantener una arquitectura de red segura	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.
12.2	Establecer y mantener una arquitectura de red segura	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
12.2	Establecer y mantener una arquitectura de red segura	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantiza r una alta disponibi lidad, asegúrese de que su ELB tenga instancias registrad as de varias zonas de disponibilidad.
12.3	Administrar la infraestructura de red de forma segura	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.3	Administrar la infraestructura de red de forma segura	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.3	Administrar la infraestructura de red de forma segura	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.3	Administrar la infraestructura de red de forma segura	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.3	Administrar la infraestructura de red de forma segura	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.3	Administrar la infraestructura de red de forma segura	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.3	Administrar la infraestructura de red de forma segura	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.3	Administrar la infraestructura de red de forma segura	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
12.6	Usar protocolos seguros de comunicación y administración de redes	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.6	Usar protocolos seguros de comunicación y administración de redes	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.6	Usar protocolos seguros de comunicación y administración de redes	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.6	Usar protocolos seguros de comunicación y administración de redes	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.6	Usar protocolos seguros de comunicación y administración de redes	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.6	Usar protocolos seguros de comunicación y administración de redes	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.6	Usar protocolos seguros de comunicación y administración de redes	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.6	Usar protocolos seguros de comunicación y administración de redes	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
13.1	Centralizar las alertas de eventos de seguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13.1	Centralizar las alertas de eventos de seguridad	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13.3	Implementar una solución de detección de intrusiones en la red	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13.6	Recopilar registros de flujo de tráfico de red	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13.6	Recopilar registros de flujo de tráfico de red	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabilitada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para CIS Critical Security Controls v8 IG2.

Mejores prácticas operativas para los controles de seguridad críticos de CIS v8 IG3

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los Controles de seguridad críticos de Center for Internet Security (CIS) v8 IG3 y las reglas de Config AWS administradas. Cada una AWS Config se aplica a un AWS recurso específico y se refiere a uno o más controles de CIS Critical Security Controls v8 IG3. Un IG3 control CIS Critical Security Controls v8 puede estar relacionado con varias AWS Config reglas. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			durante más días de los permitidos, de acuerdo con los estándares de su organización.
1.1	Establecer y mantener un inventario detallado de los activos empresariales	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.1	Establecer y mantener un inventario detallado de los activos empresariales	ec-2 security-group-attached-to -es	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Asegurarse de que el software autorizado sea compatible actualmente	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Asegurarse de que el software autorizado sea compatible actualmente	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Asegurarse de que el software autorizado o sea compatible actualmente	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.4	Utilizar herramientas automatizadas de inventario de software	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.4	Utilizar herramientas automatizadas de inventario de software	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.
3.3	Configurar listas de control de acceso a datos	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.3	Configurar listas de control de acceso a datos	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
3.3	Configurar listas de control de acceso a datos	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.3	Configurar listas de control de acceso a datos	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
3.3	Configurar listas de control de acceso a datos	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
3.3	Configurar listas de control de acceso a datos	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.3	Configurar listas de control de acceso a datos	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.3	Configurar listas de control de acceso a datos	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
3.3	Configurar listas de control de acceso a datos	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.
3.3	Configurar listas de control de acceso a datos	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).
3.3	Configurar listas de control de acceso a datos	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Configurar listas de control de acceso a datos	efs-access-point-enforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.
3.4	Hacer cumplir la retención de datos	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Hacer cumplir la retención de datos	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.
3.10	Cifrar los datos confidenciales en tránsito	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.10	Cifrar los datos confidenciales en tránsito	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.10	Cifrar los datos confidenciales en tránsito	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.10	Cifrar los datos confidenciales en tránsito	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
3.10	Cifrar los datos confidenciales en tránsito	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.10	Cifrar los datos confidenciales en tránsito	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.11	Cifrar los datos confidenciales en reposo	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
3.11	Cifrar los datos confidenciales en reposo	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
3.11	Cifrar los datos confidenciales en reposo	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
3.11	Cifrar los datos confidenciales en reposo	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.
3.11	Cifrar los datos confidenciales en reposo	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
3.11	Cifrar los datos confidenciales en reposo	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11	Cifrar los datos confidenciales en reposo	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
3.11	Cifrar los datos confidenciales en reposo	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
3.14	Acceso a datos confidenciales de los registros	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14	Acceso a datos confidenciales de los registros	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
4.1	Establecer y mantener un proceso de configuración seguro	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	efs-access-point-enforce-directorio-raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.
4.1	Establecer y mantener un proceso de configuración seguro	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Establecer y mantener un proceso de configuración seguro	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Administrar el software y los activos empresariales de forma segura	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
4.6	Administrar el software y los activos empresariales de forma segura	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Administrar el software y los activos empresariales de forma segura	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
4.6	Administrar el software y los activos empresariales de forma segura	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.6	Administrar el software y los activos empresariales de forma segura	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
4.6	Administrar el software y los activos empresariales de forma segura	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.7	Administrar las cuentas predeterminadas del software y los activos empresariales	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.1	Establecer y mantener un inventario de las cuentas	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Utilizar contraseñas únicas	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3	Deshabilitar las cuentas inactivas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4	Restringir los privilegios de administrador a las cuentas de administrador dedicadas	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4	Restringir los privilegios de administrador a las cuentas de administrador dedicadas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.6	Centralizar la administración de cuentas	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4	Requerir la MFA para el acceso remoto a la red	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4	Requerir la MFA para el acceso remoto a la red	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4	Requerir la MFA para el acceso remoto a la red	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.5	Requerir la MFA para el acceso administrativo	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.7	Centralizar el control de los accesos	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1	Establecer y mantener un proceso de administración de vulnerabilidades	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1	Establecer y mantener un proceso de administración de vulnerabilidades	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1	Establecer y mantener un proceso de administración de vulnerabilidades	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
7.3	Administrar los parches del sistema operativo de forma automática	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3	Administrar los parches del sistema operativo de forma automática	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3	Administrar los parches del sistema operativo de forma automática	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.4	Administrar los parches de las aplicaciones de forma automática	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.4	Administrar los parches de las aplicaciones de forma automática	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.4	Administrar los parches de las aplicaciones de forma automática	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.5	Realizar los escaneos automatizados de vulnerabilidades de los activos internos de la empresa	ecr-private-image-scanning-activado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identific ar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.
8.1	Establecer y mantener un proceso de administración de registros de auditoría	audit-log-policy-e xists (Verificación del proceso)	Establezca y mantenga una política de administr ación de registros de auditoría que defina los requisito s de registro de su organización. Esto incluye, pero no se limita a, la revisión y la conservación de los registros de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
8.2	Recopilar los registros de auditoría	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2	Recopilar los registros de auditoría	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3	Garantizar el almacenamiento adecuado de los registros de auditoría	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).
8.5	Recopilar registros de auditoría detallados	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
8.5	Recopilar registros de auditoría detallados	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.5	Recopilar registros de auditoría detallados	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.7	Recopilar registros de auditoría de solicitud es de URL	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.9	Centralizar los registros de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
8.10	Conservar los registros de auditoría	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.10	Conservar los registros de auditoría	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implementar y mantener un software antimalware	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2	Configurar las actualizaciones automáticas de firmas antimalware	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4	Configurar el escaneo antimalware automático de los medios extraíbles	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6	Administrar el software antimalware de forma centralizada	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7	Utilizar un software antimalware basado en el comportamiento	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	ebs-optimized-inst ance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operation s. This optimization provides the most efficient performan ce for your EBS volumes by minimizin g contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automáticas	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	redshift-cluster-m aintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configura ción preferida para su organización. En concreto, que tengan períodos de mantenimi ento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVers ionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	Realizar copias de seguridad automátic as	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).
11.3	Proteger los datos de recuperación	backup-recovery-po int-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Proteger los datos de recuperación	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
11.3	Proteger los datos de recuperación	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Proteger los datos de recuperación	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Establecer y mantener una instancia aislada de los datos de recuperación	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
12.2	Establecer y mantener una arquitectura de red segura	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
12.2	Establecer y mantener una arquitectura de red segura	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS
12.2	Establecer y mantener una arquitectura de red segura	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
12.2	Establecer y mantener una arquitectura de red segura	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
12.2	Establecer y mantener una arquitectura de red segura	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
12.2	Establecer y mantener una arquitectura de red segura	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
12.2	Establecer y mantener una arquitectura de red segura	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.
12.2	Establecer y mantener una arquitectura de red segura	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
12.2	Establecer y mantener una arquitectura de red segura	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.2	Establecer y mantener una arquitectura de red segura	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantiza r una alta disponibi lidad, asegúrese de que su ELB tenga instancias registrad as de varias zonas de disponibilidad.
12.3	Administrar la infraestructura de red de forma segura	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.3	Administrar la infraestructura de red de forma segura	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.3	Administrar la infraestructura de red de forma segura	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.3	Administrar la infraestructura de red de forma segura	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.3	Administrar la infraestructura de red de forma segura	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.3	Administrar la infraestructura de red de forma segura	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.3	Administrar la infraestructura de red de forma segura	elb 2- acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.3	Administrar la infraestructura de red de forma segura	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
12.6	Usar protocolos seguros de comunicación y administración de redes	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.6	Usar protocolos seguros de comunicación y administración de redes	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.6	Usar protocolos seguros de comunicación y administración de redes	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.6	Usar protocolos seguros de comunicación y administración de redes	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.6	Usar protocolos seguros de comunicación y administración de redes	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.6	Usar protocolos seguros de comunicación y administración de redes	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
12.6	Usar protocolos seguros de comunicación y administración de redes	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.6	Usar protocolos seguros de comunicación y administración de redes	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
13.1	Centralizar las alertas de eventos de seguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13.1	Centralizar las alertas de eventos de seguridad	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13.3	Implementar una solución de detección de intrusiones en la red	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13.6	Recopilar registros de flujo de tráfico de red	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13.6	Recopilar registros de flujo de tráfico de red	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13.10	Filtrar la capa de aplicación	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabilitada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.12	Implementar controles de seguridad en el nivel de código	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.12	Implementar controles de seguridad en el nivel de código	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.12	Implementar controles de seguridad en el nivel de código	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabilitada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.
16.12	Implementar controles de seguridad en el nivel de código	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16.12	Implementar controles de seguridad en el nivel de código	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para CIS Critical Security Controls v8 IG3.

Prácticas operativas recomendadas para los 20 principales controles del CIS

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante AWS Config reglas gestionadas o personalizadas y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los 20 principales controles de seguridad críticos del Center for Internet Security (CIS) y las reglas de Config AWS administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más de los 20 controles principales de CIS. Un control de los 20 principales controles del CIS puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este paquete de conformidad ha sido validado por AWS Security Assurance Services LLC (AWS SAS), que está formado por un equipo de asesores de seguridad cualificados en el sector de las tarjetas de pago (QSAs), profesionales certificados por HITRUST en el marco de seguridad común (CCSFPs) y profesionales del cumplimiento certificados para ofrecer orientación y evaluaciones en relación con diversos marcos del sector. AWS Los profesionales de SAS diseñaron este paquete de conformidad para permitir a un cliente alinearse con un subconjunto de los 20 principales países de la CEI.

ID de control	AWS Config Regla	Directrices
CIS.2	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establece r líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.
CIS.2	ec2- -comprobar managedin stance-patch-compliance-sta tus	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute

ID de control	AWS Config Regla	Directrices
		Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CIS.2	ec2- -eni security-group-attached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.
CIS.2	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	AWS Config Regla	Directrices
CIS.2	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.
CIS.2	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	AWS Config Regla	Directrices
CIS.3	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CIS.3	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Config Regla	Directrices
CIS.3	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
CIS.4	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Config Regla	Directrices
CIS.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
CIS.4	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Config Regla	Directrices
CIS.4	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
CIS.4	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Config Regla	Directrices
CIS.4	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Config Regla	Directrices
CIS.5	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
CIS.5	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Config Regla	Directrices
CIS.5	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CIS.5	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Config Regla	Directrices
CIS.5	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que establezcas el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.
CIS.6	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Config Regla	Directrices
CIS.6	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
CIS.6	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Config Regla	Directrices
CIS.6	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
CIS.6	cloudtrail-s3-dataevents-en abled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la Cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Config Regla	Directrices
CIS.6	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Config Regla	Directrices
CIS.6	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
CIS.6	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Config Regla	Directrices
CIS.6	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Config Regla	Directrices
CIS.6	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrail entregará todos los archivos de registro Regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Config Regla	Directrices
CIS.6	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Config Regla	Directrices
CIS.6	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Config Regla	Directrices
CIS.6	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
CIS.6	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Config Regla	Directrices
CIS.8	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CIS.9	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CIS.9	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Config Regla	Directrices
CIS.9	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
CIS.9	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearc h Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Config Regla	Directrices
CIS.9	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
CIS.9	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Config Regla	Directrices
CIS.9	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Config Regla	Directrices
CIS.9	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
CIS.9	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Config Regla	Directrices
CIS.9	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Config Regla	Directrices
CIS.9	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CIS.9	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Config Regla	Directrices
CIS.9	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
CIS.9	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Config Regla	Directrices
CIS.9	bloques s3 account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
CIS.9	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Config Regla	Directrices
CIS.9	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CIS.9	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
CIS.9	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Config Regla	Directrices
CIS.9	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Config Regla	Directrices
CIS.10	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.
CIS.10	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	AWS Config Regla	Directrices
CIS.10	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.
CIS.10	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Config Regla	Directrices
CIS.10	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.
CIS.11	ec2- -eni security-group-attached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.

ID de control	AWS Config Regla	Directrices
CIS.11	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Config Regla	Directrices
CIS.11	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.
CIS.11	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Config Regla	Directrices
CIS.11	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
CIS.12	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Config Regla	Directrices
CIS.12	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CIS.12	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Config Regla	Directrices
CIS.12	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
CIS.12	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Config Regla	Directrices
CIS.12	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CIS.12	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Config Regla	Directrices
CIS.12	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Config Regla	Directrices
CIS.12	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
CIS.12	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Config Regla	Directrices
CIS.12	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Config Regla	Directrices
CIS.12	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CIS.12	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Config Regla	Directrices
CIS.12	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
CIS.12	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Config Regla	Directrices
CIS.12	bloques s3 account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
CIS.12	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Config Regla	Directrices
CIS.12	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CIS.12	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Config Regla	Directrices
CIS.12	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
CIS.12	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Config Regla	Directrices
CIS.12	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
CIS.13	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Config Regla	Directrices
CIS.13	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CIS.13	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
CIS.13	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
CIS.13	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Config Regla	Directrices
CIS.13	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CIS.13	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
CIS.13	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Config Regla	Directrices
CIS.13	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
CIS.13	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
CIS.13	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Config Regla	Directrices
CIS.13	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
CIS.13	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Config Regla	Directrices
CIS.13	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Config Regla	Directrices
CIS.13	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
CIS.13	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Config Regla	Directrices
CIS.13	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
CIS.13	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
CIS.13	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Config Regla	Directrices
CIS.13	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
CIS.13	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Config Regla	Directrices
CIS.13	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
CIS.14	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Config Regla	Directrices
CIS.14	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CIS.14	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
CIS.14	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
CIS.14	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Config Regla	Directrices
CIS.14	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CIS.14	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CIS.14	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Config Regla	Directrices
CIS.14	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
CIS.14	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
CIS.14	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Config Regla	Directrices
CIS.14	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Config Regla	Directrices
CIS.14	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Config Regla	Directrices
CIS.14	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
CIS.14	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	AWS Config Regla	Directrices
CIS.14	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CIS.14	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Config Regla	Directrices
CIS.14	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
CIS.14	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Config Regla	Directrices
CIS.14	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
CIS.14	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Config Regla	Directrices
CIS.14	s3- -bloques account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
CIS.14	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Config Regla	Directrices
CIS.14	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
CIS.14	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CIS.14	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Config Regla	Directrices
CIS.14	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
CIS.14	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CIS.14	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Config Regla	Directrices
CIS.14	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
CIS.14	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Config Regla	Directrices
CIS.16	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Config Regla	Directrices
CIS.16	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Config Regla	Directrices
CIS.16	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Config Regla	Directrices
CIS.16	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Config Regla	Directrices
CIS.16	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CIS.16	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Config Regla	Directrices
CIS.16	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y la referencia fundamental de seguridad de las contraseñas de los Centros para la Seguridad de Internet (CIS AWS). Esta regla le permite configurar opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS funda mentales: verdadero), RequireSymbols (valor de las mejores prácticas de seguridad AWS funda mentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad

ID de control	AWS Config Regla	Directrices
		AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
CIS.16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegi o y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Config Regla	Directrices
CIS.16	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
CIS.16	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Config Regla	Directrices
CIS.16	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
CIS.16	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Config Regla	Directrices
CIS.16	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Config Regla	Directrices
CIS.16	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
CIS.16	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Config Regla	Directrices
CIS.16	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
CIS.16	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	AWS Config Regla	Directrices
CIS.16	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
CIS.16	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Config Regla	Directrices
CIS.18	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.
CIS.18	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild . AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	AWS Config Regla	Directrices
CIS.19	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
CIS.19	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Config Regla	Directrices
CIS.19	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Config Regla	Directrices
CIS.2	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

Plantilla

La plantilla está disponible en GitHub: Las 20 mejores prácticas operativas para el CIS.

Prácticas operativas recomendadas para CISA Cyber Essentials

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre las reglas de Cyber Essentials (CE) de la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA) y las reglas de Config AWS gestionadas. Cada AWS Config regla se aplica a un AWS recurso específico y se refiere a uno o

más controles CE de la CISA. Un control CISA CE puede estar relacionado con varias AWS Config reglas. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Staff-1	Desarrollar una cultura de concienci a para alentar al personal a tomar buenas decisiones en línea.	security-awareness -program-exists(Ve rificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infraccio nes o incidentes de seguridad.
Your Staff-2	Obtener informaci ón sobre riesgos como la suplantac ión de identidad y el compromiso con el correo electrónico de la empresa.XXXXX.	security-awareness -program-exists(Ve rificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infraccio nes o incidentes de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Staff-3	Estar al corriente de los eventos actuales relacionados con la ciberseguridad mediante la aplicación de las lecciones aprendidas y los eventos notificados para mantenerse alerta ante el entorno de amenazas actual y adaptarse a las tendencias de ciberseguridad.	security-awareness-program-exists(Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
Your Staff-4	Aprovechar la formación básica sobre ciberseguridad para mejorar la exposición a los conceptos, la terminología y las actividades de ciberseguridad asociados con la implementación de las prácticas recomendadas de ciberseguridad.	security-awareness-program-exists(Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Staff-5	Identificar los recursos de formación disponibles a través de asociaciones profesionales, instituciones académicas, el sector privado y fuentes gubernamentales.	security-awareness-program-exists(Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
Your Systems-1	Saber lo que hay en la red. Realizar inventarios de los activos de hardware y software para saber qué hay en juego y puede ser atacado.	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-1	Saber lo que hay en la red. Realizar inventarios de los activos de hardware y software para saber qué hay en juego y puede ser atacado.	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-1	Saber lo que hay en la red. Realizar inventarios de los activos de hardware y software para saber qué hay en juego y puede ser atacado.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-1	Saber lo que hay en la red. Realizar inventarios de los activos de hardware y software para saber qué hay en juego y puede ser atacado.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-1	Saber lo que hay en la red. Realizar inventarios de los activos de hardware y software para saber qué hay en juego y puede ser atacado.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
Your Systems-1	Saber lo que hay en la red. Realizar inventarios de los activos de hardware y software para saber qué hay en juego y puede ser atacado.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-1	Saber lo que hay en la red. Realizar inventarios de los activos de hardware y software para saber qué hay en juego y puede ser atacado.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-2	Aprovechar las actualizaciones automáticas de todos los sistemas operativos y el software externo.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-2	Aprovechar las actualizaciones automáticas de todos los sistemas operativos y el software externo.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-2	Aprovechar las actualizaciones automáticas de todos los sistemas operativos y el software externo.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-2	Aprovechar las actualizaciones automáticas de todos los sistemas operativos y el software externo.	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	api-gw-cache-enabledy cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	opensearch-data-node-fault-tolerancia	Amazon OpenSearch Service (OpenSearch Servicio) requiere al menos tres nodos de datos para una alta disponibilidad y tolerancia a errores. La implementación de un dominio OpenSearch de servicio con al menos tres nodos de datos garantiza las operaciones del clúster en caso de que un nodo falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
Your Systems-3	Implementar configura ciones de seguridad para todos los activos de hardware y software.	rds-snapshot-encry pted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	secretsmanager-secret-periodic-rotation	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación periódica . La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	secretsmanager-secret-unused	Si existen credenciales no utilizadas en AWS Secrets Manager, debe deshabilitar la opción and/or Eliminar las credenciales, ya que esto podría infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedForDays (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-3	Implementar configuraciones de seguridad para todos los activos de hardware y software.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Systems-4	Eliminar el hardware y el software no compatibles o no autorizados de los sistemas.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-1	Saber quién está en su red. Realice inventarios de las conexiones de red (usuarios, proveedores, socios comerciales, etc.).	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-1	Saber quién está en su red. Realice inventarios de las conexiones de red (usuarios, proveedores, socios comerciales, etc.).	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
Your Surroundings-1	Saber quién está en su red. Realice inventarios de las conexiones de red (usuarios, proveedores, socios comerciales, etc.).	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-2	Aprovechar la autenticación de varios factores para todos los usuarios, empezando por los usuarios con privilegios, administrativos y de acceso remoto.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-2	Aprovechar la autenticación de varios factores para todos los usuarios, empezando por los usuarios con privilegios, administrativos y de acceso remoto.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-2	Aprovechar la autenticación de varios factores para todos los usuarios, empezando por los usuarios con privilegios, administrativos y de acceso remoto.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-2	Aprovechar la autenticación de varios factores para todos los usuarios, empezando por los usuarios con privilegios, administrativos y de acceso remoto.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-3	Otorgue permisos de acceso y administr ación en función del need-to-know privilegi o mínimo.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-3	Otorgue permisos de acceso y de administrador en need-to-know función del privilegio mínimo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-3	Otorgue permisos de acceso y administración en función del need-to-know privilegio mínimo.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Your Surroundings-3	Otorgue permisos de acceso y de administrador en need-to-know función del privilegio mínimo.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-3	Otorgue permisos de acceso y administr ación en función del need-to-know privilegi o mínimo.	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-3	Otorgue permisos de acceso y administr ación en función del privilegio mínimo need-to-know.	secretsmanager-sec ret-unused	Si existen credencia les no utilizadas en AWS Secrets Manager, debe deshabilitar la opción and/or Eliminar las credenciales, ya que esto podría infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedFor Days (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-3	Otorgue permisos de acceso y de administrador en need-to-know función del privilegio mínimo.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearch Permite un control de acceso al dominio basado en funciones, así como una seguridad a nivel de índices, documentos y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Surroundings-4	Aprovechar las contraseñas únicas para todos los usuarios.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. AWS Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
Your Data-1	Saber cómo se protegen sus datos.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
Your Data-1	Saber cómo se protegen sus datos.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
Your Data-1	Saber cómo se protegen sus datos.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
Your Data-1	Saber cómo se protegen sus datos.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
Your Data-1	Saber cómo se protegen sus datos.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
Your Data-1	Saber cómo se protegen sus datos.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
Your Data-1	Saber cómo se protegen sus datos.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Your Data-1	Saber cómo se protegen sus datos.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Your Data-1	Saber cómo se protegen sus datos.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-1	Saber cómo se protegen sus datos.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Your Data-1	Saber cómo se protegen sus datos.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	api-gw-cache-enabl ed-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	opensearch-encrypt ed-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	codebuild-project-source-repo-Verificación de URL	Asegúrese de que la URL del repositor io fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorizac ión de acceso a los repositorios de Bitbucket GitHub .
Your Data-2	Descubre lo que sucede en tu red. Gestiona los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y el comportamiento de los usuarios.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Gestione los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Gestione los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y el comportamiento de los usuarios.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Gestione los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Gestione los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, y las actividades en tránsito data-at-rest y del comportamiento de los usuarios.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividades en tránsito y del comportamiento de los usuarios.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-2	Conozca lo que sucede en su red. Administre los componentes de la red y el perímetro, los componentes del host y del dispositivo, data-at-rest y las actividad es en tránsito y del comportamiento de los usuarios.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-3	Proteger el sistema de nombres de dominio.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-4	Establecer copias de seguridad automatizadas y redundancias periódicas de los sistemas clave.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Data-5	Aprovechar las protecciones para las copias de seguridad, incluidas la seguridad física, el cifrado y las copias fuera de línea.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Your Data-5	Aprovechar las protecciones para las copias de seguridad, incluidas la seguridad física, el cifrado y las copias fuera de línea.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Crisis Response-2	Dirigir el desarrollo de una estructura de informes internos para detectar, comunicar y contener los ataques.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Your Crisis Response-2	Dirigir el desarrollo de una estructura de informes internos para detectar, comunicar y contener los ataques.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-1	Emplear una solución de copia de seguridad que respalde de manera automática y continua los datos esenciales y las configuraciones del sistema.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-2	Exigir la autentica ción multifactor (MFA) para acceder a los sistemas siempre que sea posible. La MFA debe ser obligatoria para todos los usuarios, pero comience con los usuarios con privilegi os, administrativos y de acceso remoto.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-2	Exigir la autenticación multifactor (MFA) para acceder a los sistemas siempre que sea posible. La MFA debe ser obligatoria para todos los usuarios, pero comience con los usuarios con privilegios, administrativos y de acceso remoto.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-2	Exigir la autenticación multifactor (MFA) para acceder a los sistemas siempre que sea posible. La MFA debe ser obligatoria para todos los usuarios, pero comience con los usuarios con privilegios, administrativos y de acceso remoto.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-2	Exigir la autenticación multifactor (MFA) para acceder a los sistemas siempre que sea posible. La MFA debe ser obligatoria para todos los usuarios, pero comience con los usuarios con privilegios, administrativos y de acceso remoto.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-3	Activar las actualizaciones automáticas siempre que sea posible. Sustituir los sistemas operativos, las aplicaciones y el hardware no compatibles. Probar e implementar los parches rápidamente.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-3	Activar las actualizaciones automáticas siempre que sea posible. Sustituir los sistemas operativos, las aplicaciones y el hardware no compatibles. Probar e implementar los parches rápidamente.	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-3	Activar las actualizaciones automáticas siempre que sea posible. Sustituir los sistemas operativos, las aplicaciones y el hardware no compatibles. Probar e implementar los parches rápidamente.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
Booting Up: Things to Do First-3	Activar las actualizaciones automáticas siempre que sea posible. Sustituir los sistemas operativos, las aplicaciones y el hardware no compatibles. Probar e implementar los parches rápidamente.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para CISA Cyber Essentials.

Prácticas operativas recomendadas para los Servicios de Información de la Justicia Criminal (CJIS, por sus siglas en inglés)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los requisitos de cumplimiento de los Servicios de Información de Justicia Penal (CJIS) y las reglas de Config AWS administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles CJIS. Un control de los CJIS puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.2	Formación de concienciación sobre la seguridad	security-awareness -program-exists (Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infraccio nes o incidentes de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3	Respuesta frente a incidencias	response-plan-exists-maintained (Verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable. Contar con planes de respuesta actualizados y documentados formalmente puede ayudar a garantizar que el personal de respuesta comprenda los roles, responsabilidades y procesos que deben seguirse durante un incidente.
5.3	Respuesta frente a incidencias	response-plan-tested (Verificación del proceso)	Asegúrese de que se prueben los planes de respuesta y recuperación ante incidentes. Esto puede ayudar a comprender si su plan será efectivo durante un incidente y si es necesario abordar alguna laguna o actualización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4	Auditoría y rendición de cuentas	audit-log-policy-exists (Verificación del proceso)	Establezca y mantenga una política de administración de registros de auditoría que defina los requisitos de registro de su organización. Esto incluye, pero no se limita a, la revisión y la conservación de los registros de auditoría.
5.4.1	Eventos y contenido auditables (sistemas de información)	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
5.4.1	Eventos y contenido auditables (sistemas de información)	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.
5.4.1	Eventos y contenido auditables (sistemas de información)	codebuild-project-sCifrado con 3 registros	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para AWS CodeBuild los registros almacenados en Amazon S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.1	Eventos y contenido auditables (sistemas de información)	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
5.4.1	Eventos y contenido auditables (sistemas de información)	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.5	Protección de la información de auditoría	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.5	Protección de la información de auditoría	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.5	Protección de la información de auditoría	codebuild-project-sCifrado con 3 registros	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para AWS CodeBuild los registros almacenados en Amazon S3.
5.4.6	Retención de los registros de auditoría	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.4.6	Retención de los registros de auditoría	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
5.5.2	Aplicación de normas de acceso	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalm ente RequireUp percaseCharacters (valor de CJIS: falso), RequireLo wercaseCharacters (valor de CJIS: falso), RequireSy mbols (valor de CJIS: falso), RequireNu mbers (valor de CJIS: falso), MinimumPa sswordLength (valor de CJIS: 8),

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			PasswordReusePrevention (valor de CJIS: 10) y MaxPasswordAge (valor de CJIS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.
5.5.2	Aplicación de normas de acceso	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	rds-instance-iam-authentication-habilitado	Asegúrese de que la autenticación AWS Identity and Access Management (IAM) esté habilitada en las instancias del Amazon Relational Database Service (Amazon RDS) para controlar el acceso a los sistemas y activos. De esta manera se fuerza el cifrado del tráfico de red hacia y desde la base de datos mediante la capa de sockets seguros (SSL). No es necesario almacenar credenciales de usuario en la base de datos, ya que la autenticación se administra de forma externa.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2	Aplicación de normas de acceso	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabilitada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.™
5.5.2.1	Privilegio mínimo	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
5.5.2.1	Privilegio mínimo	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
5.5.2.1	Privilegio mínimo	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	ecs-containers-non privileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.
5.5.2.1	Privilegio mínimo	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	efs-access-point-enforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.2.1	Privilegio mínimo	secretsmanager-secret-unused	Si existen credenciales no utilizadas en AWS Secrets Manager, debe deshabilitar la opción and/or Eliminar las credenciales, ya que esto podría infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedForDays (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.6	Acceso remoto	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.5.6	Acceso remoto	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.6.2.1.1	Contraseña	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalm ente RequireUp percaseCharacters (valor de CJIS: falso), RequireLo wercaseCharacters (valor de CJIS: falso), RequireSy mbols (valor de CJIS: falso), RequireNu mbers (valor de CJIS: falso), MinimumPa sswordLength (valor de CJIS: 8), PasswordReusePreve

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ntion (valor de CJIS: 10) y MaxPasswo rdAge (valor de CJIS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.6.2.2	Autenticación avanzada	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
5.6.2.2	Autenticación avanzada	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.6.2.2	Autenticación avanzada	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.6.2.2	Autenticación avanzada	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.6.2.2	Autenticación avanzada	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.6.3.1	Administración de identificadores	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
5.7.1.1	Funcionalidad mínima	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
5.7.1.1	Funcionalidad mínima	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
5.7.1.1	Funcionalidad mínima	lambda-function-pu blic-access-prohibido	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibi lidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
5.7.1.1	Funcionalidad mínima	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
5.7.1.1	Funcionalidad mínima	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
5.7.1.1	Funcionalidad mínima	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
5.7.1.1	Funcionalidad mínima	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.7.1.1	Funcionalidad mínima	subnet-auto-assign-public-ip-deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.
5.10	Protección de sistemas y comunicaciones e integridad de la información	alb-http-drop-invalid-habilitado para encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicaciones e integridad de la información	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicaciones e integridad de la información	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicac iones e integridad de la información	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
5.10	Protección de sistemas y comunicac iones e integridad de la información	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicaciones e integridad de la información	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicaciones e integridad de la información	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicaciones e integridad de la información	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicaciones e integridad de la información	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicaciones e integridad de la información	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicaciones e integridad de la información	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10	Protección de sistemas y comunicaciones e integridad de la información	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.
5.10	Protección de sistemas y comunicaciones e integridad de la información	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
5.10.1	Aplicación del flujo de información	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
5.10.1	Aplicación del flujo de información	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
5.10.1	Aplicación del flujo de información	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
5.10.1	Aplicación del flujo de información	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
5.10.1	Aplicación del flujo de información	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
5.10.1	Aplicación del flujo de información	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
5.10.1	Aplicación del flujo de información	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
5.10.1	Aplicación del flujo de información	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
5.10.1	Aplicación del flujo de información	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
5.10.1	Aplicación del flujo de información	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1	Aplicación del flujo de información	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.1	Protección perimetral	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.1	Protección perimetral	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.1	Protección perimetral	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
5.10.1.1	Protección perimetral	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.1	Protección perimetral	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.1	Protección perimetral	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.1	Protección perimetral	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
5.10.1.1	Protección perimetral	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.1	Protección perimetral	waf-regional-rule-not-vacío	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencadenar un comportamiento no deseado.
5.10.1.1	Protección perimetral	waf-regional-rulegroup-not-vacío	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportamiento no deseado.
5.10.1.1	Protección perimetral	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitud es web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
5.10.1.2	Cifrado	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
5.10.1.2	Cifrado	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
5.10.1.2	Cifrado	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus AWS CloudTrail registros.
5.10.1.2	Cifrado	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	codebuild-project-sCifrado con 3 registros	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para AWS CodeBuild los registros almacenados en Amazon S3.
5.10.1.2	Cifrado	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
5.10.1.2	Cifrado	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
5.10.1.2	Cifrado	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
5.10.1.2	Cifrado	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
5.10.1.2	Cifrado	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.
5.10.1.2	Cifrado	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
5.10.1.2	Cifrado	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
5.10.1.2	Cifrado	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
5.10.1.2	Cifrado	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
5.10.1.2	Cifrado	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.2	Cifrado	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.3	Herramientas y técnicas de detección de intrusos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.3	Herramientas y técnicas de detección de intrusos	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.1.3	Herramientas y técnicas de detección de intrusos	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.4.1	Administración de parches	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.4.1	Administración de parches	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.4.1	Administración de parches	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.4.1	Administración de parches	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administr ación de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independi entes de sus servicios para usar la versión de plataforma más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.4.1	Administración de parches	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.4.4	Alertas y avisos de seguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.4.4	Alertas y avisos de seguridad	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.10.4.4	Alertas y avisos de seguridad	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el CJIS.

Prácticas operativas recomendadas para la CMMC 2.0 de nivel 1

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el

cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre la certificación del modelo de madurez de ciberseguridad (CMMC) 2.0 de nivel 1 y las reglas de Config AWS administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de nivel 1 de CMMC 2.0. Un control de la CMMC 2.0 de nivel 1 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizad os para garantiza r que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomenda da de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven compromet idas. Esta regla requiere un valor de rotación de clave

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	s3- bucket-level-publi c-access -prohibido	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
AC.L1-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC.L1-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC.L1-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- -bloques-periódico s account-level-public-access	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictPublicBuck ets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-level-publi c-access -prohibido	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifica control/limit las conexiones y el uso de sistemas de información externos.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
AC.L1-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifica control/limit las conexiones y el uso de sistemas de información externos.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	s3-: bucket-level-public-access prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L1-3.1.20	Verifique control/limit las conexiones y el uso de sistemas de información externos.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	api-gw-execution-l ogging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.
IA.L1-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de información.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L1-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	alb-http-drop-inva lid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	s3- bucket-level-publi c-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L1-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L1-3.14.1	Identificar, notificar y corregir los defectos de la información y de los sistemas de información de manera oportuna.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L1-3.14.1	Identificar, notificar y corregir los defectos de la información y de los sistemas de información de manera oportuna.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L1-3.14.1	Identificar, notificar y corregir los defectos de la información y de los sistemas de información de manera oportuna.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L1-3.14.2	Proporcionar protección contra código malicioso en las ubicaciones adecuadas dentro de los sistema de información de la organización.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L1-3.14.5	Realizar análisis periódicos del sistema de información y análisis en tiempo real de los archivos de orígenes externos cuando se descargan , abren o ejecutan archivos.	ecr-private-image-scanning-habilitado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identific ar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para la CMMC 2.0 de nivel 1.

Prácticas operativas recomendadas para la CMMC 2.0 de nivel 2

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre la certificación del modelo de madurez de ciberseguridad (CMMC) 2.0 de nivel 2 y las reglas de Config AWS administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles CMMC 2.0

de nivel 2. Un control de la CMMC 2.0 de nivel 2 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizad os para garantiza r que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomenda da de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven compromet idas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube. AWS Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	s3- -bloques-periódico s account-level-public-access	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictPublicBuck ets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	secretsmanager-rot ation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencial mente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
AC.L2-3.1.1	Limitar el acceso al sistema de información a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas de información).	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.1	Limitar el acceso al sistema de informaci ón a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas de informaci ón).	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC.L2-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube. AWS Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
AC.L2-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- -bloques-periódico s account-level-public-access	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictPublicBuck ets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC.L2-3.1.2	Limitar el acceso al sistema de información a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.2	Limitar el acceso al sistema de informaci ón a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.20	Verificar control/limit las conexiones y el uso de sistemas de información externos.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	ssm-document-not-p ublic	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y capturen la ejecución de dichas funciones en los registros de auditoría.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.12	Monitorear y controlar las sesiones de acceso remoto.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.12	Monitorear y controlar las sesiones de acceso remoto.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
AC.L2-3.1.12	Monitorear y controlar las sesiones de acceso remoto.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.12	Monitorear y controlar las sesiones de acceso remoto.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC.L2-3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo, los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.1	Crear y retener los registros de auditoría del sistema y los registros si son necesarios para habilitar el monitoreo, los análisis, la investigación y la gestión de informes de actividad del sistema ilegal o no autorizada.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	api-gw-execution-l ogging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.
AU.L2-3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.2	Garantizar que las acciones de usuarios del sistema individuales se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.4	Alertar sobre el evento de un error en el proceso de registro de auditoría.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.4	Alertar sobre el evento de un error en el proceso de registro de auditoría.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
AU.L2-3.3.4	Alertar sobre el evento de un error en el proceso de registro de auditoría.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.4	Alertar sobre el evento de un error en el proceso de registro de auditoría.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.5	Relacionar los procesos de revisión, análisis y gestión de informes de auditoría para investigar y responder a los indicios de actividad poco usual, sospechosa, no autorizada o ilegal.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.5	Relacionar los procesos de revisión, análisis y gestión de informes de auditoría para investigar y responder a los indicios de actividad poco usual, sospechosa, no autorizada o ilegal.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
AU.L2-3.3.8	Proteger la informaci ón de auditoría y las herramien tas de registro de auditoría de todo acceso, modificac ión y eliminación no autorizadas.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU.L2-3.3.8	Proteger la información de auditoría y las herramientas de registro de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
CA.L2-3.12.2	Desarrollar e implementar planes de acción designados para corregir deficiencias y reducir o eliminar vulnerabilidades en los sistemas organizativos.	vuln-management-plan-exists (Verificación del proceso)	Garantizar que se desarrolle e implemente un plan de administración de vulnerabilidades para disponer de procesos bien definidos para abordar las vulnerabilidades de su entorno. Esto puede incluir herramientas de administración de vulnerabilidades, cadencia de análisis del entorno, roles y responsabilidades.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA.L2-3.12.3	Monitorear los controles de seguridad de forma continua para garantizar una eficiencia continua de los controles.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA.L2-3.12.3	Monitorear los controles de seguridad de forma continua para garantizar una eficiencia continua de los controles.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA.L2-3.12.3	Monitorear los controles de seguridad de forma continua para garantizar una eficiencia continua de los controles.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.1	Establecer y mantener configuraciones de referencia e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectivos.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.1	Establecer y mantener configuraciones de referencia e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectivos.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
CM.L2-3.4.1	Establecer y mantener configuraciones de referencia e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectivos.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.1	Establecer y mantener configura ciones de referenci a e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectiv os.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.1	Establecer y mantener configura ciones de referenci a e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectiv os.	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizado s EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	account-part-of-or ganizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantiza r que las cuentas cumplan con las normas. La falta de gobernanza centraliz ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrai l entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	ec2- -check managedinstance-as sociation-compliance-status	Use AWS Systems Manager Associati ons para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancia s administradas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	ec2- -check managedinstance-pa tch-compliance-status	Habilite esta regla para ayudar a identific ar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimi entos de su organizac ión en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	elastic-beanstalk-managed-updates-ha bilitado	La activación de las actualizaciones de plataforma gestionad as para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correccio nes, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomenda da para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	rds-automatic-mino r-version-habilitada para la actualización	Habilite las actualiza ciones automátic as de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundari as del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correccio nes de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	redshift-cluster-m aintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configura ción preferida para su organización. En concreto, que tengan períodos de mantenimi ento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrad e El valor predeterm inado es true. También te permite configurar de forma opcional el periodo preferredMaintenan ceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
CM.L2-3.4.2	Establecer y forzar los ajustes de configura ción de la seguridad para los productos de tecnología de la información empleados en los sistema organizativos.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.3	Rastrear, revisar, autorizar o desautorizar y registrar los cambios en los sistemas organizativos.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube aseguránd ose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidenc ialidad de los sistemas. Esta regla le permite configura r de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,338 9,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ssm-document-not-p ublic	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube aseguránd ose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	autoscaling-launch-config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.7	Restringir, deshabilitar o evitar el uso de programas, funciones, puertos, protocolos y servicios no esenciales.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.9	Controlar y monitorear el software instalado por el usuario.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.9	Controlar y monitorear el software instalado por el usuario.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM.L2-3.4.9	Controlar y monitorear el software instalado por el usuario.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
IA.L2-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de información.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
IA.L2-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.1	Identificar los usuarios, los procesos que actúan en nombre de los usuarios o los dispositivos del sistema de informaci ón.	wafv2-logging-enabled	Para facilitar el registro y la supervisi ón en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la informaci ón sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube. AWS Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de información de la organización.	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.3	Usar la autenticación multifactor para el acceso local y de red a cuentas con privilegios y para el acceso de red a cuentas sin privilegios.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.3	Usar la autenticación multifactor para el acceso local y de red a cuentas con privilegios y para el acceso de red a cuentas sin privilegios.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.3	Usar la autenticación multifactor para el acceso local y de red a cuentas con privilegios y para el acceso de red a cuentas sin privilegios.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.3	Usar la autenticación multifactor para el acceso local y de red a cuentas con privilegios y para el acceso de red a cuentas sin privilegios.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.6	Deshabilitar los identificadores tras un período definido de inactividad.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.6	Deshabilitar los identificadores tras un período definido de inactividad.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.7	Forzar una complejidad de contraseña mínima y cambiar los caracteres cuando se crean nuevas contraseñas.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.8	Prohibir la reutilización de contraseñas para un número específico de generaciones.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñ as protegidas criptográficamente.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñ as protegidas criptográficamente.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA.L2-3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR.L2-3.6.1	Establecer una capacidad operativa de gestión de incidentes para los sistemas organizativos que incluya actividad es de preparación, detección, análisis, contención, recuperac ión y respuesta del usuario.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR.L2-3.6.1	Establecer una capacidad operativa de gestión de incidentes para los sistemas organizativos que incluya actividades de preparación, detección, análisis, contención, recuperación y respuesta del usuario.	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR.L2-3.6.1	Establecer una capacidad operativa de gestión de incidentes para los sistemas organizativos que incluya actividad es de preparación, detección, análisis, contención, recuperac ión y respuesta del usuario.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR.L2-3.6.1	Establecer una capacidad operativa de gestión de incidentes para los sistemas organizativos que incluya actividad es de preparación, detección, análisis, contención, recuperac ión y respuesta del usuario.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR.L2-3.6.3	Probar la capacidad operativa de respuesta ante incidentes.	response-plan-tested (Verificación del proceso)	Asegúrese de que se prueben los planes de respuesta y recuperación ante incidentes. Esto puede ayudar a comprender si su plan será efectivo durante un incidente y si es necesario abordar alguna laguna o actualización.
MA.L2-3.7.5	Requerir la autenticación multifactor para establecer sesiones de mantenimiento no locales a través de conexiones de red externas y finalizar dichas conexiones cuando se complete el mantenimiento no local.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
MA.L2-3.7.5	Requerir la autenticación multifactor para establecer sesiones de mantenimiento no locales a través de conexiones de red externas y finalizar dichas conexiones cuando se complete el mantenimiento no local.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA.L2-3.11.2	Analizar en busca de vulnerabilidades de los sistemas organizativos y las aplicaciones de forma periódica y al identificar nuevas vulnerabilidades que afecten a dichos sistemas y aplicaciones.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA.L2-3.11.2	Analizar en busca de vulnerabilidades de los sistemas organizativos y las aplicaciones de forma periódica y al identificar nuevas vulnerabilidades que afecten a dichos sistemas y aplicaciones.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA.L2-3.11.2	Analizar en busca de vulnerabilidades de los sistemas organizativos y las aplicaciones de forma periódica y al identificar nuevas vulnerabilidades que afecten a dichos sistemas y aplicaciones.	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA.L2-3.11.2	Analizar en busca de vulnerabilidades de los sistemas organizativos y las aplicaciones de forma periódica y al identificar nuevas vulnerabilidades que afecten a dichos sistemas y aplicaciones.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.1	Monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de información.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	dms-replication-not-public	Gestiona el acceso a la AWS nube asegurándote de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involunta ria a través de los recursos compartidos del sistema.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involunta ria a través de los recursos compartidos del sistema.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.4	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	alb-http-drop-invalid-encabezado activado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC.L2-3.13.10	Establecer y administrar claves criptográficas para la criptografía empleada en los sistemas organizativos.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.10	Establecer y administrar claves criptográficas para la criptografía empleada en los sistemas organizativos.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.15	Proteger la autenticidad de las sesiones de comunicación.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC.L2-3.13.15	Proteger la autenticidad de las sesiones de comunicación.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.15	Proteger la autenticidad de las sesiones de comunicación.	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.15	Proteger la autenticidad de las sesiones de comunicación.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC.L2-3.13.15	Proteger la autenticidad de las sesiones de comunicación.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.15	Proteger la autenticidad de las sesiones de comunicación.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	api-gw-cache-enabledy cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
SC.L2-3.13.16	Proteger la confidencialidad de la CUI en reposo.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.1	Identificar, notificar y corregir los defectos de la información y de los sistemas de información de manera oportuna.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.1	Identificar, notificar y corregir los defectos de la información y de los sistemas de información de manera oportuna.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.1	Identificar, notificar y corregir los defectos de la información y de los sistemas de información de manera oportuna.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.2	Proporcionar protección contra código malicioso en las ubicaciones adecuadas dentro de los sistema de información de la organización.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.5	Realizar análisis periódicos del sistema de información y análisis en tiempo real de los archivos de orígenes externos cuando se descargan , abren o ejecutan archivos.	ecr-private-image-scanning-habilitado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identific ar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.6	Monitorear los sistemas organizat ivos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI.L2-3.14.7	Identificar el uso no autorizado de sistemas organizativos.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para la CMMC 2.0 de nivel 2.

Prácticas operativas recomendadas para servicios de computación

Este paquete de conformidad contiene AWS Config reglas basadas en los servicios de cómputo. Para obtener más información, consulte Informática para cualquier carga de trabajo. Para ver una lista de todas las reglas administradas compatibles AWS Config, consulta la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para servicios de computación.

Prácticas operativas recomendadas para la resiliencia de datos

Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para la resiliencia de los datos.

Prácticas operativas recomendadas para servicios de bases de datos

Este paquete de conformidad contiene AWS Config reglas basadas en los servicios de bases de datos. Para obtener más información, consulte Bases de datos en AWS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para los servicios de bases de datos.

Prácticas operativas recomendadas para lagos de datos y servicios de análisis

Este paquete de conformidad contiene reglas de AWS Config para lagos de datos y servicios de análisis. Para obtener más información, consulte Lagos de datos y análisis en AWS. Para ver una lista de las reglas administradas por AWS Config, consulte List of AWS Config Managed Rules.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Operational Best Practices for Data Lakes and Analytics Services.

Mejores prácticas operativas para DevOps

Este paquete de conformidad contiene AWS Config reglas basadas DevOps en AWS ellas. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para DevOps.

Prácticas operativas recomendadas para EC2

Este paquete de conformidad contiene AWS Config reglas basadas en EC2. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para EC2.

Prácticas operativas recomendadas para el cifrado y la administración de claves

Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para el cifrado y la gestión de claves.

Prácticas operativas recomendadas para la guía de ciberseguridad para pymes de la ENISA

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear comprobaciones de control de seguridad, operativas o de optimización de costos mediante reglas de AWS Config administradas o personalizadas y acciones correctivas de AWS Config. Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para

garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación se proporciona un ejemplo de asignación entre la guía de ciberseguridad para pymes de la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés) y las reglas de AWS Config administradas. Cada regla de Config se aplica a un recurso de AWS específico que está relacionado con uno o más controles de la guía de ciberseguridad para pymes de la ENISA. Un control de la guía de ciberseguridad para pymes de la ENISA puede relacionarse con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones de controles adaptados de la guía de ciberseguridad para pymes de la ENISA. La guía de ciberseguridad para pymes de la ENISA está disponible en Guía de ciberseguridad para pymes: 12 pasos para proteger su empresa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: PUBLICAR POLÍTICAS DE CIBERSEGURIDAD	Deben definirse reglas claras y específicas en materia de ciberseguridad	security-awareness-program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD:	En virtud del Reglamento General de Protección de Datos1 de la UE,	autoscaling-launch-config-public-ip-disabled	Si configura las interfaces de red con una dirección IP pública, se

ID de control	Descripción del control	Regla de AWS Config	Directrices
RECORDAR LA PROTECCIÓN DE DATOS	todas las pymes que traten o almacenen datos personale s de residentes en la UE o el EEE deben garantiza r que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantiza r que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.		puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicación de DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	ebs-snapshot-public-restorable-check	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	ec2-instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	emr-master-no-public-ip	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	lambda-function-public-access-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	rds-instance-public-access-check	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	redshift-cluster-public-access-check	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	s3-account-level-public-access-blocks-periodic	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterminado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	s3-bucket-level-public-access-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	s3-bucket-public-read-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	s3-bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	s3-bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACL) se utilizan para el control de acceso en los buckets de Amazon S3. Las ACL son mecanismos de control de acceso heredados para buckets de Amazon S3 que sean anteriores a AWS Identity and Access Management (IAM). En lugar de las ACL, se recomienda utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	subnet-auto-assign-public-ip-disabled	Gestione el acceso a la nube de AWS de manera que garantice que no se asigne automáticamente una dirección IP pública a las subredes de Amazon Virtual Private Cloud (VPC). Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	alb-http-to-https-redirection-check	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	alb-http-drop-invalid-header-enabled	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	api-gw-cache-enabled-and-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos de recuperación de AWS Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	backup-recovery-point-manual-deletion-disabled	Asegúrese de que los puntos de recuperación de AWS Backup tengan adjunta una política basada en los recursos que impida eliminar los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se cifran con una clave maestra de cliente (CMK) propiedad de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	ec2-ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	elasticsearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon Elasticsearch Service (Amazon ES).

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	efs-access-point-enforce-root-directory	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	efs-access-point-enforce-user-identity	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en el Amazon Elastic File System (Amazon EFS). Cuando está habilitada, Amazon EFS reemplaza los ID de usuario y grupo del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario obligatoria.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	cloud-trail-log-file-validation-enabled	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para sus artefactos de AWS CodeBuild.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para los secretos de AWS Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	codebuild-project-s3-logs-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para los registros de AWS CodeBuild almacenados en Amazon S3.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	opensearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	elasticsearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	opensearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	elb-tls-https-listeners-only	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar certificados SSL/TLS públicos y privados con servicios de AWS y recursos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	elbv2-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar certificados SSL/TLS públicos y privados con servicios de AWS y recursos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	internet-gateway-authorized-vpc-only	Gestione el acceso a recursos en la nube de AWS de manera que garantice que las puertas de enlace de Internet solo se conecten a la Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a internet para las cargas de trabajo dentro de las Amazon VPC puede reducir el acceso no deseado a su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	s3-default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	s3-bucket-server-side-encryption-enabled	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	s3-bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	sagemaker-endpoint-configuration-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenciales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	sagemaker-notebook-instance-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenciales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	sagemaker-notebook-no-direct-internet-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1_DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD: RECORDAR LA PROTECCIÓN DE DATOS	En virtud del Reglamento General de Protección de Datos1 de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE o el EEE deben garantizar que se realicen los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2_IMPARTIR FORMACIÓN ADECUADA	Imparta formación periódica sobre concienciación en materia de ciberseguridad a todo el personal, a fin de garantizar que puedan reconocer y hacer frente a las distintas amenazas informáticas. Estas formaciones deben adaptarse a las pymes y centrarse en situaciones de la vida real. Imparta formación especializada sobre ciberseguridad a los responsables de la gestión de la ciberseguridad en la empresa, a fin de garantizar que posean los conocimientos y las competencias necesarios para ejercer su trabajo.	security-awareness-program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4_DESARROLLAR UN PLAN DE RESPUESTA ANTE INCIDENTES	Desarrolle un plan formal de respuesta ante incidentes que incluya directrices claras, funciones y responsabilidades documentadas para garantizar que todos los incidentes de seguridad reciban una respuesta oportuna, profesional y adecuada. Para responder de forma rápida a las amenazas de seguridad, busque herramientas que permitan controlar y crear alertas cuando se detecte alguna actividad sospechosa o fallos de seguridad.	response-plan-exists-maintained (verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable.

ID de control	Descripción del control	Regla de AWS Config	Directrices
5_PROTEGER EL ACCESO A LOS SISTEMAS	Anime a todo el mundo a utilizar una frase de contraseña, una combinación de al menos tres palabras corrientes escogidas de forma aleatoria que formen una frase fácil de memorizar y segura. Si decide utilizar una contraseña corriente: Si opta por una contraseña típica: - Asegúrese de que sea larga, con caracteres en mayúscula y minúscula y, a ser posible, números y caracteres especiales. - Evite palabras obvias, como “contraseña”, secuencias de letras o números como “abc” o “123”. - No utilice información personal que se pueda encontrar en línea. Y, tanto si utiliza contraseñas como frases	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de contraseña: - No las comparta con sus colegas. - Habilite la autentica ción multifactor. - Utilice un administr ador de contraseñas dedicado.		básica de AWS: true), RequireNu mbers (valor de Prácticas recomenda das de seguridad básica de AWS: true), MinimumPa sswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordR eusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñ as de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
5_PROTEGER EL ACCESO A LOS SISTEMAS	Anime a todo el mundo a utilizar una frase de contraseña, una combinación de al menos tres palabras corrientes escogidas de forma aleatoria que formen una frase fácil de memorizar y segura. Si decide utilizar una contraseña corriente: Si opta por una contraseña típica: - Asegúrese de que sea larga, con caracteres en mayúscula y minúscula y, a ser posible, números y caracteres especiales. - Evite palabras obvias, como “contraseña”, secuencias de letras o números como “abc” o “123”. - No utilice información personal que se pueda encontrar en línea. Y, tanto si utiliza contraseñas como frases	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de contraseña: - No las comparta con sus colegas. - Habilite la autentica ción multifactor. - Utilice un administr ador de contraseñas dedicado.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
5_PROTEGER EL ACCESO A LOS SISTEMAS	Anime a todo el mundo a utilizar una frase de contraseña, una combinación de al menos tres palabras corrientes escogidas de forma aleatoria que formen una frase fácil de memorizar y segura. Si decide utilizar una contraseña corriente: Si opta por una contraseña típica: - Asegúrese de que sea larga, con caracteres en mayúscula y minúscula y, a ser posible, números y caracteres especiales. - Evite palabras obvias, como “contraseña”, secuencias de letras o números como “abc” o “123”. - No utilice información personal que se pueda encontrar en línea. Y, tanto si utiliza contraseñas como frases	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de contraseña: - No las comparta con sus colegas. - Habilite la autentica ción multifactor. - Utilice un administr ador de contraseñas dedicado.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
5_PROTEGER EL ACCESO A LOS SISTEMAS	Anime a todo el mundo a utilizar una frase de contraseña, una combinación de al menos tres palabras corrientes escogidas de forma aleatoria que formen una frase fácil de memorizar y segura. Si decide utilizar una contraseña corriente: Si opta por una contraseña típica: - Asegúrese de que sea larga, con caracteres en mayúscula y minúscula y, a ser posible, números y caracteres especiales. - Evite palabras obvias, como “contraseña”, secuencias de letras o números como “abc” o “123”. - No utilice información personal que se pueda encontrar en línea. Y, tanto si utiliza contraseñas como frases	root-account-hardware-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de contraseña: - No las comparta con sus colegas. - Habilite la autentica ción multifactor. - Utilice un administr ador de contraseñas dedicado.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
5_PROTEGER EL ACCESO A LOS SISTEMAS	Anime a todo el mundo a utilizar una frase de contraseña, una combinación de al menos tres palabras corrientes escogidas de forma aleatoria que formen una frase fácil de memorizar y segura. Si decide utilizar una contraseña corriente: Si opta por una contraseña típica: - Asegúrese de que sea larga, con caracteres en mayúscula y minúscula y, a ser posible, números y caracteres especiales. - Evite palabras obvias, como “contraseña”, secuencias de letras o números como “abc” o “123”. - No utilice información personal que se pueda encontrar en línea. Y, tanto si utiliza contraseñas como frases	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de contraseña: - No las comparta con sus colegas. - Habilite la autentica ción multifactor. - Utilice un administr ador de contraseñas dedicado.		
6_PROTEGER LOS DISPOSITI VOS: MANTENER EL SOFTWARE A PUNTO Y ACTUALIZADO	Lo ideal sería utilizar una plataform a centralizada para gestionar los parches. Se recomienda encarecid amente a las pymes que: - Actualice n periódicamente todo su software. - Activen las actualiza ciones automátic as siempre que sea posible. - Identifiq uen el software y el hardware que requieren actualiza ciones manuales. - Tenga en cuenta los dispositivos móviles y de IoT.	ec2-managedinstanc e-association-comp liance-status-check	Use AWS Systems Manager Associati ons para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancia s administradas y le permite establecer líneas de referenci a de los niveles de parches del sistema operativo, las instalaci ones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: MANTENER EL SOFTWARE A PUNTO Y ACTUALIZADO	Lo ideal sería utilizar una plataforma a centralizada para gestionar los parches. Se recomienda encarecidamente a las pymes que: - Actualicen periódicamente todo su software. - Activen las actualizaciones automáticas siempre que sea posible. - Identifiquen el software y el hardware que requieren actualizaciones manuales. - Tenga en cuenta los dispositivos móviles y de IoT.	ec2-managedinstance-patch-compliance-status-check	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: MANTENER EL SOFTWARE A PUNTO Y ACTUALIZADO	Lo ideal sería utilizar una plataforma centralizada para gestionar los parches. Se recomienda encarecidamente a las pymes que: - Actualicen periódicamente todo su software. - Activen las actualizaciones automáticas siempre que sea posible. - Identifiquen el software y el hardware que requieren actualizaciones manuales. - Tenga en cuenta los dispositivos móviles y de IoT.	ec2-instance-managed-by-systems-manager	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: MANTENER EL SOFTWARE A PUNTO Y ACTUALIZADO	Lo ideal sería utilizar una plataforma a centralizada para gestionar los parches. Se recomienda encarecidamente a las pymes que: - Actualicen periódicamente todo su software. - Activen las actualizaciones automáticas siempre que sea posible. - Identifiquen el software y el hardware que requieren actualizaciones manuales. - Tenga en cuenta los dispositivos móviles y de IoT.	ecs-fargate-latest-platform-version	Las actualizaciones y los parches de seguridad se implementan automáticamente para las tareas de AWS Fargate. Si se encuentra un problema de seguridad que afecta a una versión de la plataforma de AWS Fargate, AWS parchea la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de los servicios para utilizar la versión de plataforma más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: MANTENER EL SOFTWARE A PUNTO Y ACTUALIZADO	Lo ideal sería utilizar una plataforma centralizada para gestionar los parches. Se recomienda encarecidamente a las pymes que: - Actualicen periódicamente todo su software. - Activen las actualizaciones automáticas siempre que sea posible. - Identifiquen el software y el hardware que requieren actualizaciones manuales. - Tenga en cuenta los dispositivos móviles y de IoT.	elastic-beanstalk-managed-updates-enabled	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: MANTENER EL SOFTWARE A PUNTO Y ACTUALIZADO	Lo ideal sería utilizar una plataforma centralizada para gestionar los parches. Se recomienda encarecidamente a las pymes que: - Actualicen periódicamente todo su software. - Activen las actualizaciones automáticas siempre que sea posible. - Identifiquen el software y el hardware que requieren actualizaciones manuales. - Tenga en cuenta los dispositivos móviles y de IoT.	rds-automatic-minor-version-upgrade-enabled	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: MANTENER EL SOFTWARE A PUNTO Y ACTUALIZADO	Lo ideal sería utilizar una plataforma centralizada para gestionar los parches. Se recomienda encarecidamente a las pymes que: - Actualicen periódicamente todo su software. - Activen las actualizaciones automáticas siempre que sea posible. - Identifiquen el software y el hardware que requieren actualizaciones manuales. - Tenga en cuenta los dispositivos móviles y de IoT.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure allowVersionUpgrade. El valor predeterminado es true. También le permite definir de forma opcional los parámetros preferredMaintenanceWindow (el valor predeterminado es sat:16:00-sat:16:30) y automatedSnapshotRetentionPeriod (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	api-gw-cache-enabl ed-and-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos de recuperación de AWS Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	cloud-trail-log-file-validation-enabled	Utilice la validació n de los archivos de registro de AWS CloudTrail para comprobar la integrida d de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar , eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitad o para sus grupos de registros de Amazon CloudWatch.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para sus artefactos de AWS CodeBuild.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	codebuild-project-s3-logs-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para los registros de AWS CodeBuild almacenad os en Amazon S3.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurarse de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuertos, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediendo a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se cifran con una clave maestra de cliente (CMK) propiedad de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	ec2-ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	efs-encrypted-check	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurarse de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuertos, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediendo a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	elasticsearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon Elasticsearch Service (Amazon ES).

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar certificados SSL/TLS públicos y privados con servicios de AWS y recursos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	elbv2-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar certificados SSL/TLS públicos y privados con servicios de AWS y recursos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	opensearch-encrypt ed-at-rest	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	elasticsearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticse arch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurarse de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuertos, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediendo a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	opensearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	opensearch-https-r equired	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, asegúrese de que HTTPS esté activado para las conexiones en sus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	secretsmanager-usi ng-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para los secretos de AWS Secrets Manager. Puesto que puede haber datos confidenc iales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurarse de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuertos, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediendo a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurarse de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuertos, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediendo a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	s3-bucket-server-side-encryption-enabled	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	s3-default-encryption-kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	sagemaker-endpoint -configuration-kms- key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenc iales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	sagemaker-notebook -instance-kms-key- configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenc iales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	alb-http-to-https-redirection-check	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	elb-tls-https-listeners-only	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
6_PROTEGER LOS DISPOSITIVOS: CIFRADO	Utilice el cifrado para proteger los datos. Las pymes deben asegurars e de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— estén cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuert os, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediend o a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras	s3-bucket-ssl-requ ests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	se transfiere a través de internet.		
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidenc ialidad de los sistemas. Esta regla le permite configura r de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,338 9,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	vpc-default-security-group-closed	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicacio nes web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	api-gw-associated-with-waf	AWS WAF permite configurar un conjunto de reglas (denomina das lista de control de acceso web (ACL web) que permiten, bloquean o cuentan solicitudes web en función de las reglas y condicion es de seguridad web personalizables que defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	netfw-policy-rule-group-associated	Una política de AWS Network Firewall define la forma en que su firewall monitorea y gestiona el tráfico en una Amazon VPC. Puede configurar grupos de reglas sin y con estado para filtrar los paquetes y los flujos de tráfico, y definir la administr ación del tráfico predeterminado.
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	netfw-stateless-rule-group-not-empty	Un grupo de reglas de AWS Network Firewall contiene reglas que definen cómo el firewall procesa el tráfico en la VPC. Un grupo de reglas sin estado vacío, cuando está presente en una política de firewall, no procesa el tráfico.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	waf-regional-rule-not-empty	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencadenar un comportamiento no deseado.
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	waf-regional-rulegroup-not-empty	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportamiento no deseado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: USAR FIREWALLS	Los firewalls gestionan el tráfico que entra y sale de una red y constituy en una herramien ta fundamental para proteger los sistemas de las pymes. Los firewalls deben implementarse para proteger todos los sistemas importantes; en particular, se debe utilizar un firewall para proteger la red de la pyme en internet.	waf-regional-webacl-not-empty	Una ACL web asociada a un AWS WAF puede contener una colección de reglas y grupos de reglas para inspeccio nar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireLowercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireSy mbols (valor de Prácticas recomenda das de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	root-account-hardw are-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	root-account-mfa-e nabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	api-gw-execution-l ogging-enabled	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	cloud-trail-cloud-watch-logs-enabled	Utilice Amazon CloudWatch para recopilar y administr ar de forma centraliz ada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su Cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon Elasticsearch Service tengan los registros de errores habilitad os y que se transmita n a los registros de Amazon CloudWatc h para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las Cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y que se transmitan a los registros de Amazon CloudWatch para su retención y respuesta . Los registros de errores de OpenSearch Service pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	s3-bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector , Amazon Macie, AWS Identity and Access Managemen t (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	wafv2-logging-enab led	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	cloudwatch-alarm-a ction-check	Las alarmas de Amazon CloudWatc h avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluació n. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActi onRequired (valor predeterminado de Config: True), insuffici entDataActionRequi red (valor predeterm inado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
7_PROTEGER SU RED: REVISAR LAS SOLUCIONES DE ACCESO REMOTO	Las pymes deben revisar periódica mente todas las herramientas de acceso remoto para garantizar su seguridad, en particular: - Asegurars e de que todo el software de acceso remoto tiene instalado s todos los parches y está actualiza do. - Restringir el acceso remoto desde ubicaciones geográfic as sospechosas o determinadas direcciones IP. - Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo. - Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación multifact or. - Asegurarse de que esté activado un	redshift-enhanced-vpc-routing-enabled	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	sistema de control y alertas para avisar de posibles ataques o de actividad es sospechosas extrañas.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	aurora-resources-p rotected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	backup-plan-min-fr equency-and-min-re tention-check	Para ayudar con los procesos de copia de seguridad de datos, asegúrese de que su plan de AWS Backup esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establece r los parámetros requiredFrequencyV alue (valor predeterm inado de Config: 1), requiredRetentionD ays (valor predeterm inado de Config: 35) y

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		requiredFrequencyUnit (valor predeterminado de Config: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	backup-recovery-po int-encrypted	Asegúrese de que el cifrado esté activado en sus puntos de recuperación de AWS Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperación de desastres, como los ataques de programas ransomware. Deben aplicarse las siguientes normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producción de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	backup-recovery-point-manual-deletion-disabled	Asegúrese de que los puntos de recuperación de AWS Backup tengan adjunta una política basada en los recursos que impida eliminar los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperación de desastres, como los ataques de programas ransomware. Deben aplicarse las siguientes normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producción de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	backup-recovery-point-minimum-retention-check	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus puntos de recuperación de AWS Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (valor predeterminado de Config: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	dynamodb-in-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus tablas de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperación de desastres, como los ataques de programas ransomware. Deben aplicarse las siguientes normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producción de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	ebs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperación de desastres, como los ataques de programas ransomware. Deben aplicarse las siguientes normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producción de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	ec2-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	efs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administr ado con una solución de copia de seguridad basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	elasticache-redis-cluster-automatic-backup-check	Cuando se habilitan las copias de seguridad automátic as, Amazon ElastiCac he crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperación de desastres, como los ataques de programas ransomware. Deben aplicarse las siguientes normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producción de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	fsx-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus sistemas de archivos de Amazon FSx formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperación de desastres, como los ataques de programas ransomware. Deben aplicarse las siguientes normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producción de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	rds-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un plan de AWSBackup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperación de desastres, como los ataques de programas ransomware. Deben aplicarse las siguientes normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producción de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
9_PROTEGER LAS COPIAS DE SEGURIDAD	Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperac ión de desastres, como los ataques de programas ransomware. Deben aplicarse las siguiente s normas a las copias de seguridad: - La copia de seguridad se creará periódicamente y, a ser posible, de forma automática. - La copia de seguridad estará separada del entorno de producció n de la pyme. - Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación. - Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de	s3-bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	seguridad. Lo ideal sería realizar una prueba periódica de restauración completa de principio a fin.		
11_PROTEGER SUS SITIOS WEB	Es fundamental que las pymes se aseguren de que sus sitios web estén configurados de manera segura y de que los datos personales o la información financier a, como los datos de las tarjetas de crédito, estén debidamen te protegidos. Para ello, será necesario realizar pruebas de seguridad periódica s de los sitios web para identificar las posibles deficienc ias de seguridad y llevar a cabo revisione s frecuentes para garantizar que el sitio esté correctam ente actualizado y mantenido.	vuln-management-pl an-exists (verificación del proceso)	Garantice que se desarrolle e implemente un plan de administración de vulnerabilidades para disponer de procesos bien definidos para abordar las vulnerabi lidades de su entorno.

Plantilla

La plantilla está disponible en GitHub: Operational Best Practices for ENISA Cybersecurity guide for SMEs.

Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Bajo

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costos mediante AWS Config reglas administradas o personalizadas y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los controles del marco bajo del Esquema Nacional de Seguridad (ENS) de España y las reglas de Config AWS gestionadas. Cada regla de Config se aplica a un recurso de AWS específico que está relacionado con uno o más controles bajos del ENS de España. Un control del ENS de España puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones de controles dentro del marco bajo del ENS de España, actualizado por última vez el 23 de octubre de 2020.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con

ID de control	AWS Regla de configuración	Directrices
		una clave maestra del cliente (CMK) propia.
Anexo II 4.1.2.a); b); c)	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance -kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria : SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidenta l o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicacio nes.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado o para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.b)	ec2- -eni-periodic security-group-attached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.
Anexo II 4.1.2.b)	ec2- managedinstance-association-compliance-status -check	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.b)	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
Anexo II 4.1.2.b)	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminaci ón al finalizar una instancia . Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.b)	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.
Anexo II 4.1.2.b)	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.1.a)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
Anexo II 4.2.1.a); b)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Anexo II 4.2.4	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.5	iam-root-access-key-comprue be	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorpora r el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.5.BAJO.a)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.5.BAJO.c)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloud watch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.1	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.
Anexo II 4.3.1	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.1	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.
Anexo II 4.3.1	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.1	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.
Anexo II 4.3.2.b)	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
Anexo II 4.3.2.b)	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
Anexo II 4.3.2.b)	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
Anexo II 4.3.2.b)	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Anexo II 4.3.2.b)	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
Anexo II 4.3.2.b)	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Anexo II 4.3.2.b)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
Anexo II 4.3.2.b)	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Anexo II 4.3.2.b)	s3- bucket-public-write-prohibi ted	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
Anexo II 4.3.2.b)	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.4.c)	vuln-management-plan-exists (Verificación del proceso)	Garantizar que se desarroll e e implemente un plan de administración de vulnerabi lidades para disponer de procesos bien definidos para abordar las vulnerabi lidades de su entorno. Esto puede incluir herramientas de administración de vulnerabi lidades, cadencia de análisis del entorno, roles y responsab ilidades.
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloud watch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Anexo II 4.3.8.BAJO	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus AWS CloudTrail registros.
Anexo II 4.3.10.b)	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria : SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.10.d)	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
Anexo II 5.2.3	security-awareness-program-exists (Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.3.BAJO.a)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.6.1.c)	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild . AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Anexo II 5.7.3	sagemaker-notebook-instance -kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo II 5.7.3	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
Anexo II 5.7.3	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
Anexo II 5.7.3	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
Anexo II 5.7.3	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo II 5.7.3	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Anexo II 5.7.3	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado o para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.4	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
Anexo II 5.7.4	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.2	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
Anexo II 5.8.2	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
Art. 14.4	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
Art. 16	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
Art. 16	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
Art. 16	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
Art. 20.2	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancia s de Amazon Relational Database Service (RDS) para garantizar que estén instalada s las últimas actualizaciones de las versiones secundari as del sistema de administr ación de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	AWS Regla de configuración	Directrices
Art. 20.2	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
Art. 20.2	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
Art. 20.2	vuln-management-plan-exists (Verificación del proceso)	Garantizar que se desarroll e e implemente un plan de administración de vulnerabi lidades para disponer de procesos bien definidos para abordar las vulnerabi lidades de su entorno. Esto puede incluir herramientas de administración de vulnerabi lidades, cadencia de análisis del entorno, roles y responsab ilidades.
Art. 21.1	dynamodb-table-encrypted-km s	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
Art. 21.1	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
Art. 21.1	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Art. 21.1	sagemaker-notebook-instance -kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Art. 21.1	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Art. 21.1	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria : SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
Art. 21.1	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
Art. 21.1	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
Art. 21.1	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Art. 21.1	elb-deletion-protection-ena bled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidenta l o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicacio nes.
Art. 21.1	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Art. 21.1	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Art. 21.1	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Art. 21.1	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
Art. 22	autoscaling-launch-config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
Art. 22	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
Art. 22	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
Art. 22	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Art. 22	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
Art. 22	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearc h Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
Art. 22	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
Art. 22	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
Art. 22	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
Art. 22	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
Art. 22	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Art. 22	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
Art. 22	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Art. 22	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Art. 22	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
Art. 22	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Art. 22	s3- bucket-public-write-prohibi ted	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
Art. 22	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
Art. 22	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
Art. 22	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
Art. 22	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
Art. 23	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Art. 23	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Art. 23	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Art. 23	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Art. 23	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Art. 23	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Art. 23	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Art. 23	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
Art. 23	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Art. 23	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Art. 23	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Art. 25	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
Art. 25	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Art. 25	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Art. 25	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Art. 25	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatiz adas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantán ea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
Art. 25	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	AWS Regla de configuración	Directrices
Art. 25	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.
Art. 25	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporcio na capacidad adicional y dedicada para las operacion es de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	AWS Regla de configuración	Directrices
Art. 25	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.
Art. 25	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
Art. 25	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el Esquema Nacional de Seguridad (ENS) Low.

Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Medio

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costos mediante AWS Config reglas administradas o personalizadas y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación se proporciona un ejemplo de mapeo entre los controles del marco Medium del Esquema Nacional de Seguridad (ENS) de España y las reglas de Config AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de ENS

Medium de España. Un control del ENS de España puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones de controles dentro del marco medio del ENS de España, actualizado por última vez el 23 de octubre de 2020.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
Anexo II 4.1.2.a); b); c)	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS

ID de control	AWS Regla de configuración	Directrices
		1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance -kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidenta l o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicacio nes.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.b)	ec2- -eni-periodic security-group-attached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.
Anexo II 4.1.2.b)	ec2- managedinstance-association-compliance-status -check	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.b)	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
Anexo II 4.1.2.b)	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminaci ón al finalizar una instancia . Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.b)	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.
Anexo II 4.1.2.b)	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.1.a)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
Anexo II 4.2.1.a); 4.2.1.b)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Anexo II 4.2.4	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.5	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.5.a)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.5.c)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.c)	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.c)	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.c)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Anexo II 4.2.6.c)	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Anexo II 4.2.6.c)	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.c)	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Anexo II 4.2.6.c)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Anexo II 4.2.6.c)	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.c)	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.c)	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Anexo II 4.2.6.c)	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.7	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
Anexo II 4.2.7	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.7	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
Anexo II 4.2.7	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.1	ec2- -eni-periodic security-group-attached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.
Anexo II 4.3.1	ec2- managedinstance-association-compliance-status -check	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.1	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
Anexo II 4.3.1	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminaci ón al finalizar una instancia . Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.1	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.
Anexo II 4.3.1	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.
Anexo II 4.3.2.b)	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
Anexo II 4.3.2.b)	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearc h Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
Anexo II 4.3.2.b)	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Anexo II 4.3.2.b)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
Anexo II 4.3.2.b)	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Anexo II 4.3.2.b)	s3- bucket-public-write-prohibi ted	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
Anexo II 4.3.2.b)	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.4.c)	vuln-management-plan-exists (Verificación del proceso)	Garantizar que se desarroll e e implemente un plan de administración de vulnerabi lidades para disponer de procesos bien definidos para abordar las vulnerabi lidades de su entorno. Esto puede incluir herramientas de administración de vulnerabi lidades, cadencia de análisis del entorno, roles y responsab ilidades.
Anexo II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.7.a)	response-plan-exists-maintained (Verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable. Contar con planes de respuesta actualizados y documentados formalmente puede ayudar a garantizar que el personal de respuesta comprenda los roles, responsabilidades y procesos que deben seguirse durante un incidente.
Anexo II 4.3.8	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Anexo II 4.3.8	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Anexo II 4.3.8	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Anexo II 4.3.8	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Anexo II 4.3.8	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Anexo II 4.3.8	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.10.b)	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
Anexo II 4.3.10.d)	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
Anexo II 4.6.2	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.6.2	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
Anexo II 5.2.3	security-awareness-program-exists (Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
Anexo II 5.4.2	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.2	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo II 5.4.2	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.2	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.2	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo II 5.4.2	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo II 5.4.2	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.2	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.3	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.3	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
Anexo II 5.4.3	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.3	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.3	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo II 5.4.3	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.3	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.3	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.3.a)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.6.1.c)	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Anexo II 5.7.3	sagemaker-notebook-instance -kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo II 5.7.3	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
Anexo II 5.7.3	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
Anexo II 5.7.3	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
Anexo II 5.7.3	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo II 5.7.3	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Anexo II 5.7.3	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.4	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
Anexo II 5.7.4	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.2	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
Anexo II 5.8.2	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.b)	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
Anexo II 5.8.3.b)	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.b)	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
Anexo II 5.8.3.b)	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protecció n contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.b)	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
Anexo II 5.8.3.b)	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.b)	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.b)	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.b)	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
Art. 14.4	iam-root-access-key-comprue be	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorpora r el principio de funcionalidad mínima.
Art. 16	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
Art. 16	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
Art. 16	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
Art. 20.2	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancia s de Amazon Relational Database Service (RDS) para garantizar que estén instalada s las últimas actualizaciones de las versiones secundari as del sistema de administr ación de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	AWS Regla de configuración	Directrices
Art. 20.2	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
Art. 20.2	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
Art. 20.2	vuln-management-plan-exists (Verificación del proceso)	Garantizar que se desarroll e e implemente un plan de administración de vulnerabi lidades para disponer de procesos bien definidos para abordar las vulnerabi lidades de su entorno. Esto puede incluir herramientas de administración de vulnerabi lidades, cadencia de análisis del entorno, roles y responsab ilidades.
Art. 21.1	dynamodb-table-encrypted-km s	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
Art. 21.1	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
Art. 21.1	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Art. 21.1	sagemaker-notebook-instance -kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Art. 21.1	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Art. 21.1	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
Art. 21.1	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
Art. 21.1	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
Art. 21.1	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Art. 21.1	elb-deletion-protection-ena bled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidenta l o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicacio nes.
Art. 21.1	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Art. 21.1	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Art. 21.1	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Art. 21.1	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
Art. 22	autoscaling-launch-config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
Art. 22	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
Art. 22	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Art. 22	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Art. 22	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
Art. 22	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	AWS Regla de configuración	Directrices
Art. 22	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.
Art. 22	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
Art. 22	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Art. 22	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
Art. 22	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Art. 22	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Art. 22	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
Art. 22	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Art. 22	s3- bucket-public-write-prohibi ted	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
Art. 22	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
Art. 22	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
Art. 22	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
Art. 22	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
Art. 23	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Art. 23	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Art. 23	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Art. 23	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Art. 23	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Art. 23	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Art. 23	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Art. 23	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
Art. 23	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Art. 23	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Art. 23	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
Art. 24.2	response-plan-exists-maintained (Verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable. Contar con planes de respuesta actualizados y documentados formalmente puede ayudar a garantizar que el personal de respuesta comprenda los roles, responsabilidades y procesos que deben seguirse durante un incidente.

ID de control	AWS Regla de configuración	Directrices
Art. 25	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
Art. 25	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Art. 25	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Art. 25	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Art. 25	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatiz adas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantán ea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
Art. 25	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	AWS Regla de configuración	Directrices
Art. 25	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.
Art. 25	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporcio na capacidad adicional y dedicada para las operacion es de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	AWS Regla de configuración	Directrices
Art. 25	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.
Art. 25	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
Art. 25	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el medio Esquema Nacional de Seguridad (ENS).

Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Alto

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costos mediante AWS Config reglas administradas o personalizadas y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los controles del marco superior del Esquema Nacional de Seguridad (ENS) de España y las reglas de Config AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles ENS

High de España. Un control del ENS de España puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones de controles dentro del marco alto del ENS de España, actualizado por última vez el 9 de julio de 2021.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.1.ALTO	annual-risk-assessment-performed (Verificación del proceso)	Realice una evaluación anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determinar la probabilidad y el impacto de los riesgos y and/or vulnerabilidades identificados que afectan a una organización.
4.2.1.b)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
4.2.5.ALTO.a)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de

ID de control	AWS Regla de configuración	Directrices
		acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorpora r el principio de funcionalidad mínima.
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-km s	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
Anexo II 4.1.2.a); b); c)	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
Anexo II 4.1.2.a); b); c)	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance -kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidenta l o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicacio nes.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.b)	ec2- -eni-periodic security-group-attached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.
Anexo II 4.1.2.b)	ec2- managedinstance-association-compliance-status -check	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.b)	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
Anexo II 4.1.2.b)	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminaci ón al finalizar una instancia . Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.1.2.b)	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.
Anexo II 4.1.2.b)	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.1.a)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.4	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
Anexo II 4.2.5	iam-root-access-key-comprue be	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorpora r el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.5.BAJO.a)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.5.BAJO.c)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
Anexo II 4.2.6.ALTO.b)	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.ALTO.b)	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
Anexo II 4.2.6.ALTO.b)	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.ALTO.b)	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloud watch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.6.BAJO.c)	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.1	ec2- -eni-periodic security-group-attached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.
Anexo II 4.3.1	ec2- managedinstance-association-compliance-status -check	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.1	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
Anexo II 4.3.1	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminaci ón al finalizar una instancia . Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.1	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.
Anexo II 4.3.1	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.
Anexo II 4.3.2.b)	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
Anexo II 4.3.2.b)	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
Anexo II 4.3.2.b)	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
Anexo II 4.3.2.b)	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearc h Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
Anexo II 4.3.2.b)	lambda-function-public-acce ss-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicame nte a las funciones de AWS Lambda. El acceso público puede degradar la disponibi lidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Anexo II 4.3.2.b)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
Anexo II 4.3.2.b)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.
Anexo II 4.3.2.b)	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Anexo II 4.3.2.b)	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
Anexo II 4.3.2.b)	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
Anexo II 4.3.4.c)	vuln-management-plan-exists (Verificación del proceso)	Garantizar que se desarroll e e implemente un plan de administración de vulnerabi lidades para disponer de procesos bien definidos para abordar las vulnerabi lidades de su entorno. Esto puede incluir herramientas de administración de vulnerabi lidades, cadencia de análisis del entorno, roles y responsab ilidades.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
Anexo II 4.3.7.MEDIA.a)	response-plan-exists-maintained (Verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable. Contar con planes de respuesta actualizados y documentados formalmente puede ayudar a garantizar que el personal de respuesta comprenda los roles, responsabilidades y procesos que deben seguirse durante un incidente.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Anexo II 4.3.8.BAJO	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.BAJO	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.MEDIO	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.MEDIO	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.MEDIO	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Anexo II 4.3.8.MEDIO	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Anexo II 4.3.8.MEDIO	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.MEDIO	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Anexo II 4.3.8.MEDIO	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Anexo II 4.3.8.MEDIO	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.MEDIO	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.8.MEDIO	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Anexo II 4.3.8.MEDIO	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus AWS CloudTrail registros.
Anexo II 4.3.10.b)	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.3.10.d)	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.6.2.ALTO	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
Anexo II 4.6.2.MEDIA	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.2.3	security-awareness-program-exists (Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
Anexo II 5.2.4	security-awareness-program-exists (Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
Anexo II 5.2.5	security-awareness-program-exists (Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.2.MEDIO	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.2.MEDIO	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
Anexo II 5.4.2.MEDIO	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.2.MEDIO	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.2.MEDIO	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo II 5.4.2.MEDIO	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
Anexo II 5.4.2.MEDIO	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.2.MEDIO	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.3.BAJO.a)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
Anexo II 5.4.3.MEDIO	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.3.MEDIO	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.3.MEDIO	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.3.MEDIO	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.4.3.MEDIO	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.3.MEDIO	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwat ch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
Anexo II 5.4.3.MEDIO	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.4.3.MEDIO	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.6.1.c)	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Anexo II 5.7.3	sagemaker-notebook-instance -kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo II 5.7.3	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
Anexo II 5.7.3	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
Anexo II 5.7.3	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
Anexo II 5.7.3	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo II 5.7.3	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Anexo II 5.7.3	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.3	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.7.3	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado o para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo II 5.7.4	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
Anexo II 5.7.4	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.2	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
Anexo II 5.8.2	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.MEDIO.b)	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
Anexo II 5.8.3.MEDIO.b)	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.MEDIO.b)	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
Anexo II 5.8.3.MEDIO.b)	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protecció n contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.MEDIO.b)	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
Anexo II 5.8.3.MEDIO.b)	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.MEDIO.b)	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.MEDIO.b)	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Anexo II 5.8.3.MEDIO.b)	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
Art. 14.4	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
Art. 16	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
Art. 16	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
Art. 16	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
Art. 20.2	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancia s de Amazon Relational Database Service (RDS) para garantizar que estén instalada s las últimas actualizaciones de las versiones secundari as del sistema de administr ación de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	AWS Regla de configuración	Directrices
Art. 20.2	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
Art. 20.2	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
Art. 20.2	vuln-management-plan-exists (Verificación del proceso)	Garantizar que se desarroll e e implemente un plan de administración de vulnerabi lidades para disponer de procesos bien definidos para abordar las vulnerabi lidades de su entorno. Esto puede incluir herramientas de administración de vulnerabi lidades, cadencia de análisis del entorno, roles y responsab ilidades.
Art. 21.1	dynamodb-table-encrypted-km s	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
Art. 21.1	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
Art. 21.1	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
Art. 21.1	sagemaker-notebook-instance -kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Art. 21.1	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Art. 21.1	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
Art. 21.1	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
Art. 21.1	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
Art. 21.1	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Art. 21.1	elb-deletion-protection-ena bled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidenta l o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicacio nes.
Art. 21.1	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Art. 21.1	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Art. 21.1	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Art. 21.1	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Art. 21.1	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
Art. 21.1	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
Art. 22	autoscaling-launch-config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
Art. 22	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
Art. 22	account-level-public-accesss3--bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
Art. 22	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	AWS Regla de configuración	Directrices
Art. 22	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Art. 22	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Art. 22	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Art. 22	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
Art. 22	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
Art. 22	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
Art. 22	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Art. 22	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
Art. 22	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Art. 22	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.
Art. 22	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
Art. 22	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Art. 22	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Art. 22	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
Art. 22	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
Art. 22	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
Art. 22	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
Art. 23	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Art. 23	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Art. 23	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
Art. 23	api-gw-execution-logging-ac tivado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Art. 23	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Art. 23	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Art. 23	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Art. 23	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
Art. 23	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
Art. 23	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
Art. 23	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
Art. 24.2	response-plan-exists-maintained (Verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable. Contar con planes de respuesta actualizados y documentados formalmente puede ayudar a garantizar que el personal de respuesta comprenda los roles, responsabilidades y procesos que deben seguirse durante un incidente.
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
Art. 25	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
Art. 25	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Art. 25	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Art. 25	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Art. 25	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatiz adas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantán ea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
Art. 25	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	AWS Regla de configuración	Directrices
Art. 25	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.
Art. 25	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporcio na capacidad adicional y dedicada para las operacion es de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	AWS Regla de configuración	Directrices
Art. 25	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.
Art. 25	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
Art. 25	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el Esquema Nacional de Seguridad (ENS) High.

Prácticas operativas recomendadas para la FDA Título 21 CFR Parte 11

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costos mediante reglas administradas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el Título 21 de la Parte 11 del Código de Regulaciones Federales (CFR) y las reglas de Config AWS administradas. Cada AWS Config regla se aplica a un AWS recurso específico y se refiere a uno o más controles del Título 21 del CFR, parte 11 de la FDA. Un control del Título 21 de la Parte 11 del CFR de la FDA puede estar relacionado

con múltiples reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:		plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.1	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente:	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente : (a) La validació n de los sistemas para garantizar la precisión, la fiabilida d, el rendimiento previsto constante y la capacidad de discernir los registros	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente : (a) La validació n de los sistemas para garantizar la precisión, la fiabilida d, el rendimiento previsto constante y la capacidad de discernir los registros	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	dynamodb-resources-protected-by-plan de copias de seguridad	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente : (a) La validació n de los sistemas para garantizar la precisión, la fiabilida d, el rendimiento previsto constante y la capacidad de discernir los registros	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente : (a) La validació n de los sistemas para garantizar la precisión, la fiabilida d, el rendimiento previsto constante y la capacidad de discernir los registros	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente : (a) La validació n de los sistemas para garantizar la precisión, la fiabilida d, el rendimiento previsto constante y la capacidad de discernir los registros	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(a)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (a) La validación de los sistemas para garantizar la precisión, la fiabilidad, el rendimiento previsto constante y la capacidad de discernir los registros	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	no válidos o alterados .		
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente : (c) La protección de los registros para permitir su recuperac ión precisa y rápida durante todo el período de retención de los registros.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que sus registros estén cifrados AWS CloudTrail .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	ecr-private-lifecycle-policy-configurado	Las políticas de ciclo de vida de Amazon Elastic Container Repository (ECR) permiten especificar la administración de ciclo de vida de las imágenes de un repositorio. Esto permite automatizar la limpieza de las imágenes sin utilizar, como las imágenes que vencen en función de su edad o número.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente : (c) La protección de los registros para permitir su recuperac ión precisa y rápida durante todo el período de retención de los registros.	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(c)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (c) La protección de los registros para permitir su recuperación precisa y rápida durante todo el período de retención de los registros.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electróni cos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico . Dichos procedimi entos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico . Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico . Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo dentro de Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(d)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (d) Limitar el acceso al sistema a las personas autorizadas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamen te. Dicha documenta ción de registro de auditoría se conservar á durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamen te. Dicha documenta ción de registro de auditoría se conservar á durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamen te. Dicha documenta ción de registro de auditoría se conservar á durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamen te. Dicha documenta ción de registro de auditoría se conservar á durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamen te. Dicha documenta ción de registro de auditoría se conservar á durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamen te. Dicha documenta ción de registro de auditoría se conservar á durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamen te. Dicha documenta ción de registro de auditoría se conservar á durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamen te. Dicha documenta ción de registro de auditoría se conservar á durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamente. Dicha documentación de registro de auditoría se conservará durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(e)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (e) El uso de registros de auditoría seguros, generados informáticamente y con fecha y hora para registrar de forma independiente la fecha y la hora de las entradas y acciones del operador	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que crean, modifican o eliminan registros electrónicos. Los cambios en los registros no deben ocultar la información registrada previamen te. Dicha documenta ción de registro de auditoría se conservar á durante un período al menos igual al requerido para los registros electrónicos en cuestión y estará disponible para que la agencia la revise y copie.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		Amazon VPC para gestionar correctamente el acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		deben asignarse a una VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo dentro de Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(g)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (g) El uso de controles de entidades para garantizar que solo las personas autorizadas puedan usar el sistema, firmar electrónicamente un registro, acceder al dispositivo de	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	entrada o salida de la operación o del sistema informático, alterar un registro o realizar la operación en cuestión.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(h)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (h) Uso de comprobaciones del dispositivo (por ejemplo, del terminal) para determinar, según corresponda, la validez del origen de la entrada de datos o la instrucción operativa.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(h)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (h) Uso de comprobaciones del dispositivo (por ejemplo, del terminal) para determinar, según corresponda, la validez del origen de la entrada de datos o la instrucción operativa.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(h)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (h) Uso de comprobaciones del dispositivo (por ejemplo, del terminal) para determinar, según corresponda, la validez del origen de la entrada de datos o la instrucción operativa.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(i)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deberán incluir lo siguiente: (i) Determinar que las personas que desarrollan, mantienen o utilizan sistemas de record/electronic firma electrónica cuentan con la formación, la formación y la	security-awareness-program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	experiencia necesarias para realizar las tareas que se les asignen.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		Amazon VPC para gestionar correctamente el acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantiza r que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.10(k)	Las personas que utilicen sistemas cerrados para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos, además de para garantizar que el firmante no pueda repudiar fácilmente el registro firmado por no ser auténtico. Dichos procedimientos y controles deben incluir lo siguiente: (k) El uso de controles apropiados de la documentación del sistema, incluidos: (1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para la operación y	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	el mantenimiento del sistema. (2) Procedimientos de revisión y control de cambios para mantener un registro de auditoría que documente el desarrollo y la modificación secuenciados en el tiempo de la documentación de los sistemas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	(a) Las firmas electrónicas que no se basen en datos biométricos deben: (1) Emplear al menos dos componentes de identificación distintos, como un código de identificación y una contraseña. (i) Cuando una persona ejecute una serie de firmas durante un período único y continuo de acceso controlado al sistema, la primera firma debe ejecutarse con todos los componentes de firma electrónica; las firmas posteriores deben ejecutarse con al menos un componente de firma electrónica que solo sea ejecutable y diseñado para que lo utilice únicamente una persona. (ii) Cuando una persona ejecute una o más firmas que no se hayan realizado durante un período	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	único y continuo de acceso controlado al sistema, cada firma debe ejecutarse con todos los component es de firma electróni ca. (2) Ser utilizadas únicamente por sus propietarios legítimos ; y (3) Administrarse y ejecutarse para garantizar que el intento de uso de la firma electrónica de una persona por parte de una persona que no sea su propietar io real requiera la colaboración de dos o más personas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	(a) Las firmas electrónicas que no se basen en datos biométricos deben: (1) Emplear al menos dos componentes de identificación distintos, como un código de identificación y una contraseña. (i) Cuando una persona ejecute una serie de firmas durante un período único y continuo de acceso controlado al sistema, la primera firma debe ejecutarse con todos los componentes de firma electrónica; las firmas posteriores deben ejecutarse con al menos un componente de firma electrónica que solo sea ejecutable y diseñado para que lo utilice únicamente una persona. (ii) Cuando una persona ejecute una o más firmas que no se hayan realizado durante un período	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	único y continuo de acceso controlado al sistema, cada firma debe ejecutarse con todos los component es de firma electróni ca. (2) Ser utilizadas únicamente por sus propietarios legítimos ; y (3) Administrarse y ejecutarse para garantizar que el intento de uso de la firma electrónica de una persona por parte de una persona que no sea su propietar io real requiera la colaboración de dos o más personas.		mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	(a) Las firmas electrónicas que no se basen en datos biométricos deben: (1) Emplear al menos dos componentes de identificación distintos , como un código de identificación y una contraseña. (i) Cuando una persona ejecute una serie de firmas durante un período único y continuo de acceso controlado al sistema, la primera firma debe ejecutarse con todos los componentes de firma electrónica; las firmas posterior es deben ejecutars e con al menos un componente de firma electrónica que solo sea ejecutable y diseñado para que lo utilice únicamente una persona. (ii) Cuando una persona ejecute una o más firmas que no se hayan realizado durante un período	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	único y continuo de acceso controlado al sistema, cada firma debe ejecutarse con todos los component es de firma electróni ca. (2) Ser utilizadas únicamente por sus propietarios legítimos ; y (3) Administrarse y ejecutarse para garantizar que el intento de uso de la firma electrónica de una persona por parte de una persona que no sea su propietar io real requiera la colaboración de dos o más personas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	(a) Las firmas electrónicas que no se basen en datos biométricos deben: (1) Emplear al menos dos componentes de identificación distintos , como un código de identificación y una contraseña. (i) Cuando una persona ejecute una serie de firmas durante un período único y continuo de acceso controlado al sistema, la primera firma debe ejecutarse con todos los componentes de firma electrónica; las firmas posterior es deben ejecutars e con al menos un componente de firma electrónica que solo sea ejecutable y diseñado para que lo utilice únicamente una persona. (ii) Cuando una persona ejecute una o más firmas que no se hayan realizado durante un período	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	único y continuo de acceso controlado al sistema, cada firma debe ejecutarse con todos los component es de firma electróni ca. (2) Ser utilizadas únicamente por sus propietarios legítimos ; y (3) Administrarse y ejecutarse para garantizar que el intento de uso de la firma electrónica de una persona por parte de una persona que no sea su propietar io real requiera la colaboración de dos o más personas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	(a) Las firmas electrónicas que no se basen en datos biométricos deben: (1) Emplear al menos dos componentes de identificación distintos, como un código de identificación y una contraseña. (i) Cuando una persona ejecute una serie de firmas durante un período único y continuo de acceso controlado al sistema, la primera firma debe ejecutarse con todos los componentes de firma electrónica; las firmas posteriores deben ejecutarse con al menos un componente de firma electrónica que solo sea ejecutable y diseñado para que lo utilice únicamente una persona. (ii) Cuando una persona ejecute una o más firmas que no se hayan realizado durante un período	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	único y continuo de acceso controlado al sistema, cada firma debe ejecutarse con todos los component es de firma electróni ca. (2) Ser utilizadas únicamente por sus propietarios legítimos ; y (3) Administrarse y ejecutarse para garantizar que el intento de uso de la firma electrónica de una persona por parte de una persona que no sea su propietar io real requiera la colaboración de dos o más personas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	(a) Las firmas electrónicas que no se basen en datos biométricos deben: (1) Emplear al menos dos componentes de identificación distintos , como un código de identificación y una contraseña. (i) Cuando una persona ejecute una serie de firmas durante un período único y continuo de acceso controlado al sistema, la primera firma debe ejecutarse con todos los componentes de firma electrónica; las firmas posterior es deben ejecutars e con al menos un componente de firma electrónica que solo sea ejecutable y diseñado para que lo utilice únicamente una persona. (ii) Cuando una persona ejecute una o más firmas que no se hayan realizado durante un período	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	único y continuo de acceso controlado al sistema, cada firma debe ejecutarse con todos los component es de firma electróni ca. (2) Ser utilizadas únicamente por sus propietarios legítimos ; y (3) Administrarse y ejecutarse para garantizar que el intento de uso de la firma electrónica de una persona por parte de una persona que no sea su propietar io real requiera la colaboración de dos o más personas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.2	(a) Las firmas electrónicas que no se basen en datos biométricos deben: (1) Emplear al menos dos componentes de identificación distintos, como un código de identificación y una contraseña. (i) Cuando una persona ejecute una serie de firmas durante un período único y continuo de acceso controlado al sistema, la primera firma debe ejecutarse con todos los componentes de firma electrónica; las firmas posteriores deben ejecutarse con al menos un componente de firma electrónica que solo sea ejecutable y diseñado para que lo utilice únicamente una persona. (ii) Cuando una persona ejecute una o más firmas que no se hayan realizado durante un período	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	único y continuo de acceso controlado al sistema, cada firma debe ejecutarse con todos los component es de firma electróni ca. (2) Ser utilizadas únicamente por sus propietarios legítimos ; y (3) Administrarse y ejecutarse para garantizar que el intento de uso de la firma electrónica de una persona por parte de una persona que no sea su propietar io real requiera la colaboración de dos o más personas.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicional es, como el cifrado de documentos y el uso de los estándare s de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicional es, como el cifrado de documentos y el uso de los estándare s de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	codebuild-project-sCifrado con 3 registros	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para AWS CodeBuild los registros almacenados en Amazon S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicional es, como el cifrado de documentos y el uso de los estándare s de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicional es, como el cifrado de documentos y el uso de los estándare s de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicional es, como el cifrado de documentos y el uso de los estándare s de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicional es, como el cifrado de documentos y el uso de los estándare s de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimi entos y controles diseñados para garantizar la autentici dad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicional es, como el cifrado de documentos y el uso de los estándare s de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.3	Las personas que utilicen sistemas abiertos para crear, modificar, mantener o transmitir registros electrónicos deben emplear procedimientos y controles diseñados para garantizar la autenticidad, la integridad y, cuando proceda, la confidencialidad de los registros electrónicos desde el momento de su creación hasta que se reciban. Dichos procedimientos y controles deben incluir aquellos indicados en el punto 11.10, según proceda, y medidas adicionales, como el cifrado de documentos y el uso de los estándares de firma digital adecuados para garantizar, según sea necesario según las circunstancias, la autenticidad, integrida	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	d y confidencialidad del registro.		
11.300(b)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles deben incluir: (b) garantizar que la emisión de códigos de identificación y contraseñas se compruebe, recupere o revise periódica mente (por ejemplo, para cubrir situacion es como la antigüeda d de las contraseñas).	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizad os para garantiza r que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomenda da de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven compromet idas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.300(b)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles deben incluir: (b) garantizar que la emisión de códigos de identificación y contraseñas se compruebe, recupere o revise periódica mente (por ejemplo, para cubrir situacion es como la antigüeda d de las contraseñas).	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.300(b)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles deben incluir: (b) garantizar que la emisión de códigos de identificación y contraseñas se compruebe, recupere o revise periódica mente (por ejemplo, para cubrir situacion es como la antigüeda d de las contraseñas).	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.300(b)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles deben incluir: (b) garantizar que la emisión de códigos de identificación y contraseñas se compruebe, recupere o revise periódica mente (por ejemplo, para cubrir situacion es como la antigüeda d de las contraseñas).	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.300(b)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles deben incluir: (b) garantizar que la emisión de códigos de identificación y contraseñas se compruebe, recupere o revise periódica mente (por ejemplo, para cubrir situacion es como la antigüeda d de las contraseñas).	secretsmanager-rot ation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencial mente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.300(b)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles deben incluir: (b) garantizar que la emisión de códigos de identificación y contraseñas se compruebe, recupere o revise periódica mente (por ejemplo, para cubrir situacion es como la antigüeda d de las contraseñas).	secretsmanager-sch eduled-rotation-su ccess-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribui do correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.300(d)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles incluirán: (d) El uso de medidas de seguridad en las transacciones para evitar el uso no autorizado de contraseñas y códigos de and/or identific ación, y para detectar cualquier intento de uso no autorizado de dichos códigos y denunciar de forma inmediata y urgente cualquier intento de uso no autorizad o a la unidad de seguridad del sistema y, según proceda, a la dirección de la organización.	cloud-trail-cloud-watch-Habilitado para guardar registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.300(d)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles incluirán: (d) El uso de medidas de seguridad en las transacci ones para evitar el uso no autorizado de contraseñas y códigos de and/or identificación y para detectar cualquier intento de uso no autorizado de dichos códigos y denunciar de forma inmediata y urgente a la unidad de seguridad del sistema y, según proceda, a la dirección de la organización.	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.300(d)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles incluirán: (d) El uso de medidas de seguridad en las transacciones para evitar el uso no autorizado de contraseñas y códigos de and/or identific ación y para detectar cualquier intento de uso no autorizado de dichos códigos y denunciar de manera inmediata y urgente a la unidad de seguridad del sistema y, según proceda, a la dirección de la organización.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.300(d)	Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación en combinación con contraseñas deben emplear controles para garantizar su seguridad e integrida d. Dichos controles incluirán: (d) El uso de medidas de seguridad en las transacci ones para evitar el uso no autorizad o de las contraseñ as y los códigos de and/or identific ación y para detectar cualquier intento de uso no autorizado de dichas contraseñ as y denunciarlo de forma inmediata y urgente a la unidad de seguridad del sistema y, según proceda, a la dirección de la organización.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el Título 21 del CFR, parte 11 de la FDA.

Prácticas operativas recomendadas para el FedRAMP (bajo)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costos mediante reglas administradas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los controles de bajo nivel de referencia del Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) y las reglas de Config AWS administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de FedRAMP. Un control del FedRAMP puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc ryptFrom). Los

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			valores reales deben reflejar las políticas de su organización.
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	ADMINISTRACIÓN DE CUENTAS	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.
AC-3	APLICACIÓN DE NORMAS DE ACCESO	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC-3	APLICACIÓN DE NORMAS DE ACCESO	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-3	APLICACIÓN DE NORMAS DE ACCESO	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC-3	APLICACIÓN DE NORMAS DE ACCESO	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC-3	APLICACIÓN DE NORMAS DE ACCESO	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
AC-3	APLICACIÓN DE NORMAS DE ACCESO	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-3	APLICACIÓN DE NORMAS DE ACCESO	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	APLICACIÓN DE NORMAS DE ACCESO	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.
AC-17	ACCESO REMOTO	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
AC-17	ACCESO REMOTO	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
AC-17	ACCESO REMOTO	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-17	ACCESO REMOTO	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
AC-17	ACCESO REMOTO	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC-17	ACCESO REMOTO	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC-17	ACCESO REMOTO	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
AC-17	ACCESO REMOTO	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-17	ACCESO REMOTO	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17	ACCESO REMOTO	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-2	EVENTOS DE AUDITORÍA	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	EVENTOS DE AUDITORÍA	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	CONTENIDO DE LOS REGISTROS DE AUDITORÍA	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6	REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9	PROTECCIÓN DE LA INFORMACIÓN DE AUDITORÍA	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
AU-9	PROTECCIÓN DE LA INFORMACIÓN DE AUDITORÍA	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9	PROTECCIÓN DE LA INFORMACIÓN DE AUDITORÍA	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9	PROTECCIÓN DE LA INFORMACIÓN DE AUDITORÍA	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
AU-9	PROTECCIÓN DE LA INFORMACIÓN DE AUDITORÍA	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-11	RETENCIÓN DE LOS REGISTROS DE AUDITORÍA	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-12	GENERACIÓN DE AUDITORÍAS	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	GENERACIÓN DE AUDITORÍAS	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
CA-7	MONITOREO CONTINUO	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultane idad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CA-7	MONITOREO CONTINUO	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	MONITOREO CONTINUO	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
CM-2	CONFIGURACIÓN DE REFERENCIA	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
CM-2	CONFIGURACIÓN DE REFERENCIA	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
CM-2	CONFIGURACIÓN DE REFERENCIA	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CM-2	CONFIGURACIÓN DE REFERENCIA	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CM-2	CONFIGURACIÓN DE REFERENCIA	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
CM-2	CONFIGURACIÓN DE REFERENCIA	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
CM-2	CONFIGURACIÓN DE REFERENCIA	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	CONFIGURACIÓN DE REFERENCIA	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.
CM-7	FUNCIONALIDAD MÍNIMA	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-7	FUNCIONALIDAD MÍNIMA	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-7	FUNCIONALIDAD MÍNIMA	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8	INVENTARIO DE COMPONENTES DEL SISTEMA DE INFORMACIÓN	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8	INVENTARIO DE COMPONENTES DEL SISTEMA DE INFORMACIÓN	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8	INVENTARIO DE COMPONENTES DEL SISTEMA DE INFORMACIÓN	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8	INVENTARIO DE COMPONENTES DEL SISTEMA DE INFORMACIÓN	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2	IDENTIFICACIÓN Y AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2	IDENTIFICACIÓN Y AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2	IDENTIFICACIÓN Y AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2	IDENTIFICACIÓN Y AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2	IDENTIFICACIÓN Y AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2	IDENTIFICACIÓN Y AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5	ADMINISTRACIÓN DE AUTENTICADORES	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5	ADMINISTRACIÓN DE AUTENTICA DORES	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4	GESTIÓN DE INCIDENTES	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4	GESTIÓN DE INCIDENTES	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4	GESTIÓN DE INCIDENTES	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4	GESTIÓN DE INCIDENTES	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4	GESTIÓN DE INCIDENTES	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-6	NOTIFICACIÓN DE INCIDENTES	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-6	NOTIFICACIÓN DE INCIDENTES	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-6	NOTIFICACIÓN DE INCIDENTES	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-7	ASISTENCIA DE RESPUESTA FRENTE A INCIDENTES	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-7	ASISTENCIA DE RESPUESTA FRENTE A INCIDENTES	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-7	ASISTENCIA DE RESPUESTA FRENTE A INCIDENTES	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA-5	ANÁLISIS DE VULNERABILIDADES	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA-5	ANÁLISIS DE VULNERABILIDADES	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA-5	ANÁLISIS DE VULNERABILIDADES	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-3	CICLO DE VIDA DE DESARROLLO DEL SISTEMA	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-3	CICLO DE VIDA DE DESARROLLO DEL SISTEMA	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-3	CICLO DE VIDA DE DESARROLLO DEL SISTEMA	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
SC-5	PROTECCIÓ N CONTRA DENEGACIÓN DE SERVICIO	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
SC-7	PROTECCIÓN PERIMETRAL	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
SC-7	PROTECCIÓN PERIMETRAL	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7	PROTECCIÓN PERIMETRAL	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SC-7	PROTECCIÓN PERIMETRAL	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
SC-7	PROTECCIÓN PERIMETRAL	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-7	PROTECCIÓN PERIMETRAL	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	PROTECCIÓN PERIMETRAL	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.
SC-12	ESTABLECIMIENTO Y ADMINISTRACIÓN DE CLAVES CRIPTOGRÁFICAS	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12	ESTABLECIMIENTO Y ADMINISTRACIÓN DE CLAVES CRIPTOGRÁFICAS	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12	ESTABLECIMIENTO Y ADMINISTRACIÓN DE CLAVES CRIPTOGRÁFICAS	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	PROTECCIÓN CRIPTOGRÁFICA	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	PROTECCIÓN CRIPTOGRÁFICA	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
SC-13	PROTECCIÓN CRIPTOGRÁFICA	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	PROTECCIÓN CRIPTOGRÁFICA	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	PROTECCIÓN CRIPTOGRÁFICA	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	PROTECCIÓN CRIPTOGRÁFICA	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	CORRECCIÓN DE DEFECTOS	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	CORRECCIÓN DE DEFECTOS	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	CORRECCIÓN DE DEFECTOS	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	CORRECCIÓN DE DEFECTOS	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3	CORRECCIÓN DE DEFECTOS	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3	CORRECCIÓN DE DEFECTOS	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
SI-3	CORRECCIÓN DE DEFECTOS	ecs-task-definition-memory-límite estricto	Limitar el máximo de memoria disponible para los contenedores de Amazon Elastic Container Service (ECS) garantiza que no se haga un uso indebido de los recursos en caso de que se produzca un acceso malintencionado a los contenedores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	cloud-trail-cloud-watch-registros activados	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	MONITOREO DEL SISTEMA DE INFORMACIÓN	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-5	ALERTAS, AVISOS Y DIRECTIVAS DE SEGURIDAD	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-5	ALERTAS, AVISOS Y DIRECTIVAS DE SEGURIDAD	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-5	ALERTAS, AVISOS Y DIRECTIVAS DE SEGURIDAD	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-5	ALERTAS, AVISOS Y DIRECTIVAS DE SEGURIDAD	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	GESTIÓN Y RETENCIÓN DE INFORMACIÓN	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-16	PROTECCIÓN DE LA MEMORIA	ecs-task-definition-memory-límite estricto	Limitar el máximo de memoria disponible para los contenedores de Amazon Elastic Container Service (ECS) garantiza que no se haga un uso indebido de los recursos en caso de que se produzca un acceso malintencionado a los contenedores.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para FedRAMP (Low).

Prácticas operativas recomendadas para FedRAMP (moderadas)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de control de seguridad, operativos o de optimización de costos mediante reglas administradas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) y las reglas de Config AWS administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de FedRAMP. Un control del FedRAMP puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este paquete de conformidad ha sido validado por AWS Security Assurance Services LLC (AWS SAS), que está formado por un equipo de asesores de seguridad cualificados en el sector de las

tarjetas de pago (QSAs), profesionales certificados por HITRUST en el marco de seguridad común (CCSFPs) y profesionales del cumplimiento certificados para ofrecer orientación y evaluaciones en relación con diversos marcos del sector. AWS Los profesionales de SAS diseñaron este paquete de conformidad para permitir al cliente ajustarse a un subconjunto de los controles de FedRAMP.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuentas del sistema de información.		software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(3)	El sistema de información desactiva automáticamente las cuentas de los usuarios inactivas durante 90 días.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(3)	El sistema de información desactiva automáticamente las cuentas de los usuarios inactivas durante 90 días.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilaci ón se envíen a Amazon CloudWatc h o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(7)	La organización: (a) Establece y administr a los usuarios con privilegios de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de informaci ón y los privilegios en roles; (b) Monitorea la asignación de roles con privilegios; y (c) Asume [asignación: acciones definidas por la organización] cuando las asignacio nes de roles con privilegios ya no son apropiadas. Directriz complemen taria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad os a realizar. Estos	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(7)	La organización: (a) Establece y administr a los usuarios con privilegios de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de informaci ón y los privilegios en roles; (b) Monitorea la asignación de roles con privilegios; y (c) Asume [asignación: acciones definidas por la organización] cuando las asignacio nes de roles con privilegios ya no son apropiadas. Directriz complemen taria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad os a realizar. Estos	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(7)	La organización: (a) Establece y administr a los usuarios con privilegios de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de informaci ón y los privilegios en roles; (b) Monitorea la asignación de roles con privilegios; y (c) Asume [asignación: acciones definidas por la organización] cuando las asignacio nes de roles con privilegios ya no son apropiadas. Directriz complemen taria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad os a realizar. Estos	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(7)	La organización: (a) Establece y administr a los usuarios con privilegios de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de informaci ón y los privilegios en roles; (b) Monitorea la asignación de roles con privilegios; y (c) Asume [asignación: acciones definidas por la organización] cuando las asignacio nes de roles con privilegios ya no son apropiadas. Directriz complemen taria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad os a realizar. Estos	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(7)	La organización: (a) Establece y administra los usuarios con privilegios de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de información y los privilegios en roles; (b) Monitorea la asignación de roles con privilegios; y (c) Asume [asignación: acciones definidas por la organización] cuando las asignaciones de roles con privilegios ya no son apropiadas. Directriz complementaria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizados a realizar. Estos	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(7)	La organización: (a) Establece y administra los usuarios con privilegios de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de información y los privilegios en roles; (b) Monitorea la asignación de roles con privilegios; y (c) Asume [asignación: acciones definidas por la organización] cuando las asignaciones de roles con privilegios ya no son apropiadas. Directriz complementaria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizados a realizar. Estos	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		
AC-2(12)(a)	La organización: a. Monitorea las cuentas del sistema de información para detectar [asignaci ón: un uso atípico definido por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(12)(a)	La organización: a. Monitorea las cuentas del sistema de información para detectar [asignación: un uso atípico definido por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de información.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilaci ón se envíen a Amazon CloudWatc h o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de información.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	cloud-trail-cloud-watch-registros activados	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y transmitidos a Amazon CloudWatc h Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditoría s de seguridad y acceso, y pueden ayudar a diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	acm-certificate-ex piration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExp iration (valor de prácticas recomenda das de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	lambda-function-pu blic-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizac iones de acceso al sistema de informaci ón para respaldar la separación de funciones.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
AC-6(10)	El sistema de información impide que los usuarios sin privilegios ejecuten funciones con privilegios, como deshabilitar, eludir o alterar las protecciones o contramedidas de seguridad implementadas.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(10)	El sistema de información impide que los usuarios sin privilegios ejecuten funciones con privilegios, como deshabilitar, eludir o alterar las protecciones o contramedidas de seguridad implementadas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(10)	El sistema de información impide que los usuarios sin privilegios ejecuten funciones con privilegios, como deshabilitar, eludir o alterar las protecciones o contramedidas de seguridad implementadas.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información sharing/collaboration .	autoscaling-launch-config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo dentro de Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [tarea: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información sharing/collaboration .	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información sharing/collaboration .	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilaci ón se envíen a Amazon CloudWatc h o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimiento de procesos y eventos del sistema. Para las aplicaciones web: toda la actividad del administrador, las comprobaciones de autenticación, las comprobaciones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimiento de procesos y eventos del sistema. Para las aplicaciones web: toda la actividad del administrador, las comprobaciones de autenticación, las comprobaciones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimiento de procesos y eventos del sistema. Para las aplicaciones web: toda la actividad del administrador, las comprobaciones de autenticación, las comprobaciones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilaci ón se envíen a Amazon CloudWatc h o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	cloudwatch-alarm-a ction-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluació n. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
AU-7(1)	El sistema de información permite procesar los registros de auditoría de eventos de interés en función de [asignaci ón: campos de auditoría definidos por la organización dentro de los registros de auditoría].	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-7(1)	El sistema de información permite procesar los registros de auditoría de eventos de interés en función de [asignación: campos de auditoría definidos por la organización dentro de los registros de auditoría].	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9(2)	El sistema de información hace copias de seguridad de los registros de auditoría al menos una vez por semana en un sistema o componente del sistema físicamente diferente del sistema o componente que se está auditando.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9(2)	El sistema de información hace copias de seguridad de los registros de auditoría al menos una vez por semana en un sistema o componente del sistema físicamente diferente del sistema o componente que se está auditando.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.
AU-9	El sistema de información protege la información de auditoría y las herramientas de auditoría contra todo acceso, modificación y eliminación no autorizados.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9	El sistema de información protege la información de auditoría y las herramientas de auditoría contra todo acceso, modificación y eliminación no autorizados.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9	El sistema de información protege la información de auditoría y las herramientas de auditoría contra todo acceso, modificación y eliminación no autorizados.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
AU-11	La organización conserva los registros de auditoría durante al menos 90 días para respaldar after-the-fact las investigaciones de incidentes de seguridad y cumplir con los requisitos reglamentarios y organizativos de retención de información.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilaci ón se envíen a Amazon CloudWatc h o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	wafv2-logging-enab led	Para facilitar el registro y la supervisi ón en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la informaci ón sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	api-gw-execution-l ogging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultane idad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorea r la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automátic o de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibi lidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexione s o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorear; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluació n. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	dynamodb-throughpu t-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/ write actividad que puede soportar cada tabla. DynamoDB utiliza esta informaci ón para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalm ente los parámetro s de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibi lidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	lambda-function-pu blic-access-prohibido	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibi lidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo dentro de Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	vpc-default-security- group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.
CM-7(a)	La organización: a. Configura el sistema de información para proporcionar solo las capacidades esenciales.	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-7(a)	La organización: a. Configura el sistema de información para proporcionar solo las capacidades esenciales.	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-7(a)	La organización: a. Configura el sistema de información para proporcionar solo las capacidades esenciales.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(1)	La organización actualiza el inventario de los componentes del sistema de información como parte integral de las instalaciones de componentes, desmontajes y actualizaciones del sistema de información.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(1)	La organización actualiza el inventario de los componentes del sistema de información como parte integral de las instalaciones de componentes, desmontajes y actualizaciones del sistema de información.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados de forma continua, con un retraso máximo de cinco minutos en la detección, para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados de forma continua, con un retraso máximo de cinco minutos en la detección, para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados de forma continua, con un retraso máximo de cinco minutos en la detección, para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados de forma continua, con un retraso máximo de cinco minutos en la detección, para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	aurora-resources-p rotected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalment e administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	dynamodb-resources -protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	fsx-resources-prot ected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	aurora-resources-p rotected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	dynamodb-resources -protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	ebs-resources-prot ected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	elb-cross-zone-loa d-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	fsx-resources-prot ected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	vpc-vpn-2-tunnels-up	Se pueden implement ar túneles Site-to-S ite VPN redundant es para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectivi dad en caso de que una de las conexione s Site-to-Site VPN no esté disponibl e. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)(2)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (2) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas sin privilegios.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)(2)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (2) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas sin privilegios.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)(2)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (2) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas sin privilegios.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)(2)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (2) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas sin privilegios.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2	El sistema de información identifica y autentica de forma única a los usuarios de la organización (o los procesos que actúan en nombre de los usuarios de la organización).	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2	El sistema de información identifica y autentica de forma única a los usuarios de la organización (o los procesos que actúan en nombre de los usuarios de la organización).	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5(1)(a)(d)(e)	Para la autentica ción basada en contraseñas, el sistema de informaci ón: a. Aplica una complejidad mínima de las contraseñ as con [asignación: requisitos definidos por la organización en cuanto a la distinció n entre mayúsculas y minúsculas, números de caracteres, mezcla de letras mayúscula s y letras minúsculas, números y caracteres especiales, incluidos los requisitos mínimos de cada tipo]; d. Aplica las restricci ones de duración mínima y máxima de las contraseñ as de [asignación: números definidos por la organización para una vida útil mínima y máxima]; e. Prohíbe la reutilización de contraseñas durante 24 generaciones.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5(4)	La organización emplea herramientas automatizadas para determinar si los autenticadores de contraseñas son lo suficientemente seguros como para cumplir [asignación: los requisitos definidos por la organización].	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5(7)	La organización se asegura de que los autenticadores estáticos no cifrados no estén integrados en las aplicaciones o los scripts de acceso ni se almacenen en las teclas de función.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-6(1)	La organización emplea mecanismos automatizados para ayudar a denunciar los incidentes de seguridad.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-6(1)	La organización emplea mecanismos automatizados para ayudar a denunciar los incidentes de seguridad.	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-6(1)	La organización emplea mecanismos automatizados para ayudar a denunciar los incidentes de seguridad.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-7(1)	La organización emplea mecanismos automatizados para aumentar la disponibilidad de la información y el apoyo relacionados con la respuesta a los incidentes.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-7(1)	La organización emplea mecanismos automatizados para aumentar la disponibilidad de la información y el apoyo relacionados con la respuesta a los incidentes.	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-7(1)	La organización emplea mecanismos automatizados para aumentar la disponibilidad de la información y el apoyo relacionados con la respuesta a los incidentes.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA-5(1)	La organización emplea herramientas de análisis de vulnerabilidades que incluyen la capacidad de actualizar fácilmente las vulnerabilidades del sistema de información que se van a analizar. Directriz complementaria: las vulnerabilidades que se van a analizar deben actualizarse rápidamente a medida que se descubran, anuncien y desarrollen nuevos métodos de análisis. Este proceso de actualización ayuda a garantizar que las posibles vulnerabilidades del sistema de información se identifiquen y aborden lo antes posible. Controles relacionados: SI-3 y SI-7.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA-5(1)	La organización emplea herramientas de análisis de vulnerabilidades que incluyen la capacidad de actualizar fácilmente las vulnerabilidades del sistema de información que se van a analizar. Directriz complementaria: las vulnerabilidades que se van a analizar deben actualizarse rápidamente a medida que se descubran, anuncien y desarrollen nuevos métodos de análisis. Este proceso de actualización ayuda a garantizar que las posibles vulnerabilidades del sistema de información se identifiquen y aborden lo antes posible. Controles relacionados: SI-3 y SI-7.	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA-5(1)	La organización emplea herramientas de análisis de vulnerabilidades que incluyen la capacidad de actualizar fácilmente las vulnerabilidades del sistema de información que se van a analizar. Directriz complementaria: las vulnerabilidades que se van a analizar deben actualizarse rápidamente a medida que se descubran, anuncien y desarrollen nuevos métodos de análisis. Este proceso de actualización ayuda a garantizar que las posibles vulnerabilidades del sistema de información se identifiquen y aborden lo antes posible. Controles relacionados: SI-3 y SI-7.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA-5	La organización: a. Realiza análisis mensuales en busca de vulnerabilidades en el sistema de información y en las aplicaciones alojadas [system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications identifican e informan al respecto; b. Emplea herramientas y técnicas de análisis de vulnerabilidades que facilitan la interoperabilidad entre las herramientas y automatizan partes del proceso de administración de vulnerabilidades mediante el uso de estándares para: 1. Enumerar las plataformas, los defectos del software y las configuraciones incorrectas;	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	2. Formatear las listas de verificación y los procedimientos de prueba; y 3. Medir el impacto de la vulnerabilidad; c. Analiza los informes de análisis de vulnerabilidades y los resultados de las evaluaciones de control de seguridad; d. Corrige las vulnerabilidades legítimas: las vulnerabilidades de alto riesgo se mitigan en un plazo de treinta (30) días a partir de la fecha de su descubrimiento; las vulnerabilidades de riesgo moderado se mitigan en un plazo de noventa (90) días a partir de la fecha de su descubrimiento; las vulnerabilidades de bajo riesgo se mitigan en un plazo de ciento ochenta (180) días a partir de la fecha de su descubrimiento, de acuerdo con una		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	evaluación organizativa del riesgo; y e. Comparte la información obtenida del proceso de análisis de vulnerabilidades y las evaluaciones de control de seguridad con [asignación: personal o roles definidos por la organización] para ayudar a eliminar vulnerabilidades similares en otros sistemas de información (es decir, debilidades o deficiencias sistémicas).		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA-5	La organización: a. Busca vulnerabilidades en el sistema de información y en las aplicaciones alojadas [Asignación: frecuencia definida por la organización de and/or forma aleatoria de acuerdo con el proceso definido por la organización] y cuando se identifican y notifican nuevas vulnerabilidades que puedan afectarlas; b system/applications . Emplea herramientas y técnicas de análisis de vulnerabilidades que facilitan la interoperabilidad entre las herramientas y automatizan partes del proceso de administración de vulnerabilidades mediante el uso de estándares para: 1. Enumerar las plataformas, los defectos del software y las configura	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ciones incorrectas; 2. Formatear las listas de verificac ión y los procedimi entos de prueba; y 3. Medir el impacto de la vulnerabi lidad; c. Analiza los informes de análisis de vulnerabilidades y los resultados de las evaluacio nes de control de seguridad; d. Corrige las vulnerabilidades legítimas [asignación: tiempos de respuesta definidos por la organización], de acuerdo con una evaluación organizat iva del riesgo; y e. Comparte la informaci ón obtenida del proceso de análisis de vulnerabilidades y las evaluaciones de control de seguridad con [asignación: personal o roles definidos por la organización] para ayudar a eliminar vulnerabilidades		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	similares en otros sistemas de información (es decir, debilidades o deficiencias sistémicas).		
SA-3(a)	La organización: a. Administra el sistema de información mediante [asignación: el ciclo de vida de desarrollo del sistema definido por la organización] que incorpora consideraciones de seguridad de la información.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-3(a)	La organización: a. Administra el sistema de información mediante [asignación: el ciclo de vida de desarrollo del sistema definido por la organización] que incorpora consideraciones de seguridad de la información.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-3(a)	La organización: a. Administra el sistema de información mediante [asignación: el ciclo de vida de desarrollo del sistema definido por la organización] que incorpora consideraciones de seguridad de la información.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-10	La organización exige al desarrollador del sistema de información, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el desarrollo, la implementación y el funcionamiento del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d. Documente los cambios aprobados	guardduty-non-arch ived-findings	Amazon le GuardDuty ayuda a comprende r el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasifica ciones para determina r las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-10	La organización exige al desarrollador del sistema de informaci ón, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el desarrollo, la implementación y el funcionamiento del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d. Documente los cambios aprobados	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-10	La organización exige al desarrollador del sistema de informaci ón, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el desarrollo, la implementación y el funcionamiento del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d. Documente los cambios aprobados	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-10	La organización exige al desarrollador del sistema de informaci ón, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el desarrollo, la implementación y el funcionamiento del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d. Documente los cambios aprobados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de informaci ón.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de informaci ón.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizac iones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de informaci ón.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de informaci ón.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de información.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo dentro de Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	elb-cross-zone-load-habilitado para el balanceo	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignaci ón: tipos de ataques de denegación de servicio definidos por la organizac ión o referencias a las fuentes de dicha información] mediante la aplicació n de [asignación: medidas de seguridad definidas por la organización].	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	autoscaling-launch-config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una mission/business necesidad de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [Asignación: frecuencia definida por la organización] y elimina las excepcion es que ya no son compatibles por una mission/business necesidad explícita. Directriz complemen	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	taria: control relaciona do: SC-8.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administrada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una mission/business necesidad de apoyo y la duración de esa necesidad; y (e) Revisa las excepciones a la política de flujo de tráfico [Asignación: frecuencia definida por la organización] y elimina las excepciones que ya no son compatibles por una mission/business necesidad explícita. Directriz complemen	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	taria: control relaciona do: SC-8.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una mission/business necesidad de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [Asignación: frecuencia definida por la organización] y elimina las excepcion es que ya no son compatibles por una mission/business necesidad explícita. Directriz complemen	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	taria: control relaciona do: SC-8.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una mission/business necesidad de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [Asignación: frecuencia definida por la organización] y elimina las excepcion es que ya no son compatibles por una mission/business necesidad explícita. Directriz complemen	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	taria: control relaciona do: SC-8.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una mission/business necesidad de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [Asignación: frecuencia definida por la organización] y elimina las excepcion es que ya no son compatibles por una mission/business necesidad explícita. Directriz complemen	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	taria: control relaciona do: SC-8.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una mission/business necesidad de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [Asignación: frecuencia definida por la organización] y elimina las excepcion es que ya no son compatibles por una mission/business necesidad explícita. Directriz complemen	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitad o para su clúster de Amazon Redshift. Puesto que puede haber datos confidenc iales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	taria: control relacionado: SC-8.		
SC-7(5)	El sistema de información de las interfaces administradas deniega el tráfico de comunicaciones de red de forma predeterminada y permite el tráfico de comunicaciones de red por excepción (es decir, deniega todo, permite por excepción). Directriz complementaria: esta mejora del control se aplica al tráfico de comunicaciones de red tanto entrante como saliente. Una política de tráfico de comunicaciones de permit-by-exception red que lo deniegue todo garantiza que solo se permitan las conexiones esenciales y aprobadas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibi lidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	wafv2-logging-enab led	Para facilitar el registro y la supervisi ón en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la informaci ón sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmiti da.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmitida.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmitida.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmiti da.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmiti da.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmiti da.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmiti da.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12	La organización establece y administra las claves criptográficas para la criptografía requerida empleada en el sistema de información de acuerdo con [asignación: requisitos definidos por la organización para la generación, distribución, almacenamiento, acceso y destrucción de claves].	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12	La organización establece y administra las claves criptográficas para la criptografía requerida empleada en el sistema de información de acuerdo con [asignación: requisitos definidos por la organización para la generación, distribución, almacenamiento, acceso y destrucción de claves].	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12	La organización establece y administra las claves criptográficas para la criptografía requerida empleada en el sistema de información de acuerdo con [asignación: requisitos definidos por la organización para la generación, distribución, almacenamiento, acceso y destrucción de claves].	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	api-gw-cache-enabled-y cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(2)	La organización emplea mecanismos automatizados como mínimo mensualmente para determinar el estado de los componentes del sistema de información con respecto a la corrección de defectos.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(2)	La organización emplea mecanismos automatizados como mínimo mensualmente para determinar el estado de los componentes del sistema de información con respecto a la corrección de defectos.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(2)	La organización emplea mecanismos automatizados como mínimo mensualmente para determinar el estado de los componentes del sistema de información con respecto a la corrección de defectos.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(2)	La organización emplea mecanismos automatizados como mínimo mensualmente para determinar el estado de los componentes del sistema de información con respecto a la corrección de defectos.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3	La organización: a. Emplea mecanismos de protección de códigos maliciosos en los puntos de entrada y salida del sistema de información para detectar y erradicar los códigos malicioso s; b. Actualiza los mecanismos de protección contra los códigos malicioso s cada vez que hay nuevas versiones disponibles, de conformidad con la política y los procedimientos de gestión de la configuración de la organización; c. Configura los mecanismos de protección contra códigos malicioso s para: 1. Realice escaneos periódico s del sistema de información [Asignación: frecuencia definida por la organización] y	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	escaneos en tiempo real de los archivos de fuentes externas en [selección (uno o más); punto final; entry/exit puntos de red] a medida que los archivos se descargan, abren o ejecutan de acuerdo con la política de seguridad de la organizac ión; y 2. [Seleccio nar (una o más): bloquear el código malicioso; poner en cuarentena el código malicioso; enviar una alerta al administr ador; [asignación: acción definida por la organizac ión]] en respuesta a la detección de código malicioso; y d. Aborda la aparición de falsos positivos durante la detección y erradicación de códigos maliciosos y su posible impacto en la disponibilidad del sistema de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	información. Directriz complementaria: los puntos de entrada y salida del sistema de información incluyen, por ejemplo, firewalls , servidores de correo electrónico, servidore s web, servidores proxy, servidores de acceso remoto, estaciones de trabajo, equipos portátile s y dispositivos móviles. Los códigos maliciosos incluyen, por ejemplo, virus, gusanos, troyanos y spyware. El código malicioso también puede codificarse en varios formatos (por ejemplo, UUENCODE o Unicode), incluirse en archivos comprimidos u ocultos y ocultarse en archivos mediante esteganografía. El código malicioso se puede transport ar por diferentes medios, como, por ejemplo, accesos		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	a la web, correo electrónico, archivos adjuntos de correo electrónico y dispositivos de almacenamiento portátiles. Las inserciones de código malicioso se producen mediante la explotación de las vulnerabilidades del sistema de información. Los mecanismos de protección contra códigos maliciosos incluyen, por ejemplo, las definiciones de firmas antivirus y las tecnologías basadas en la reputación. Existen diversas tecnologías y métodos para limitar o eliminar los efectos de los códigos maliciosos. La gestión generalizada de la configuración y los controles exhaustivos de integridad del software pueden ser eficaces para impedir la ejecución de código no autorizad		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	o. Además del off-the-shelf software comercial, también es posible que haya códigos malicioso s en el software creado a medida. Esto podría incluir, por ejemplo, bombas lógicas, puertas traseras y otros tipos de ciberataques que podrían afectar a las funciones de la organización missions/business . Los mecanismo s tradicionales de protección contra códigos maliciosos no siempre detectan dicho código. En estas situaciones, las organizaciones se basan más bien en otras medidas de seguridad, como las prácticas de codificación seguras, la gestión y el control de la configuración, los procesos de compra de confianza y las prácticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de monitoreo, para garantizar que el software no desempeñe funciones distintas de las previstas. Las organizaciones pueden determinar que, en respuesta a la detección de código malicioso, se puedan garantizar diferente s acciones. Por ejemplo, las organizac iones pueden definir acciones en respuesta a la detección de códigos maliciosos durante los análisis periódicos, acciones en respuesta a la detección de descargas maliciosa s o and/or acciones en respuesta a la detección de código malicioso al intentar abrir o ejecutar archivos. Controles relacionados: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2,		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	SI-4 y SI-7. Referencias: Publicación especial 800-83 del NIST.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3	La organización: a. Emplea mecanismos de protección de códigos maliciosos en los puntos de entrada y salida del sistema de información para detectar y erradicar los códigos malicioso s; b. Actualiza los mecanismos de protección contra los códigos malicioso s cada vez que hay nuevas versiones disponibles, de conformidad con la política y los procedimientos de gestión de la configuración de la organización; c. Configura los mecanismos de protección contra códigos malicioso s para: 1. Realice escaneos periódico s del sistema de información [Asignaci ón: frecuencia definida por la organización] y	codebuild-project-source-repo-comprobación de direcciones URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	escanee en tiempo real los archivos de fuentes externas en [selección (uno o más); punto final; entry/exit puntos de red] a medida que los archivos se descargan, abren o ejecutan de acuerdo con la política de seguridad de la organizac ión; y 2. [Seleccio nar (una o más): bloquear el código malicioso; poner en cuarentena el código malicioso; enviar una alerta al administr ador; [asignación: acción definida por la organizac ión]] en respuesta a la detección de código malicioso; y d. Aborda la aparición de falsos positivos durante la detección y erradicación de códigos maliciosos y su posible impacto en la disponibilidad del sistema de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	información. Directriz complementaria: los puntos de entrada y salida del sistema de información incluyen, por ejemplo, firewalls , servidores de correo electrónico, servidore s web, servidores proxy, servidores de acceso remoto, estaciones de trabajo, equipos portátile s y dispositivos móviles. Los códigos maliciosos incluyen, por ejemplo, virus, gusanos, troyanos y spyware. El código malicioso también puede codificarse en varios formatos (por ejemplo, UUENCODE o Unicode), incluirse en archivos comprimidos u ocultos y ocultarse en archivos mediante esteganografía. El código malicioso se puede transport ar por diferentes medios, como, por ejemplo, accesos		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	a la web, correo electrónico, archivos adjuntos de correo electrónico y dispositivos de almacenamiento portátiles. Las inserciones de código malicioso se producen mediante la explotación de las vulnerabilidades del sistema de información. Los mecanismos de protección contra códigos maliciosos incluyen, por ejemplo, las definiciones de firmas antivirus y las tecnologías basadas en la reputación. Existen diversas tecnologías y métodos para limitar o eliminar los efectos de los códigos maliciosos. La gestión generalizada de la configuración y los controles exhaustivos de integridad del software pueden ser eficaces para impedir la ejecución de código no autorizad		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	o. Además del off-the-shelf software comercial, también es posible que haya códigos malicioso s en el software creado a medida. Esto podría incluir, por ejemplo, bombas lógicas, puertas traseras y otros tipos de ciberataques que podrían afectar a las funciones de la organización missions/business . Los mecanismo s tradicionales de protección contra códigos maliciosos no siempre detectan dicho código. En estas situaciones, las organizaciones se basan más bien en otras medidas de seguridad, como las prácticas de codificación seguras, la gestión y el control de la configuración, los procesos de compra de confianza y las prácticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de monitoreo, para garantizar que el software no desempeñe funciones distintas de las previstas. Las organizaciones pueden determinar que, en respuesta a la detección de código malicioso, se puedan garantizar diferente s acciones. Por ejemplo, las organizac iones pueden definir acciones en respuesta a la detección de códigos maliciosos durante los análisis periódicos, acciones en respuesta a la detección de descargas maliciosa s o and/or acciones en respuesta a la detección de código malicioso al intentar abrir o ejecutar archivos. Controles relacionados: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2,		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	SI-4 y SI-7. Referencias: Publicación especial 800-83 del NIST.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3	La organización: a. Emplea mecanismos de protección de códigos maliciosos en los puntos de entrada y salida del sistema de información para detectar y erradicar los códigos malicioso s; b. Actualiza los mecanismos de protección contra los códigos malicioso s cada vez que hay nuevas versiones disponibles, de conformidad con la política y los procedimientos de gestión de la configuración de la organización; c. Configura los mecanismos de protección contra códigos malicioso s para: 1. Realiza escaneos periódico s del sistema de información [Asignaci ón: frecuencia definida por la organización] y	ecs-task-definition-memory-límite estricto	Limitar el máximo de memoria disponible para los contenedo res de Amazon Elastic Container Service (ECS) garantiza que no se haga un uso indebido de los recursos en caso de que se produzca un acceso malintencionado a los contenedores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	escanea en tiempo real los archivos de fuentes externas en [selección (uno o más); punto final; entry/exit puntos de red] a medida que los archivos se descargan, abren o ejecutan de acuerdo con la política de seguridad de la organizac ión; y 2. [Seleccio nar (una o más): bloquear el código malicioso; poner en cuarentena el código malicioso; enviar una alerta al administr ador; [asignación: acción definida por la organizac ión]] en respuesta a la detección de código malicioso; y d. Aborda la aparición de falsos positivos durante la detección y erradicación de códigos maliciosos y su posible impacto en la disponibilidad del sistema de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	información. Directriz complementaria: los puntos de entrada y salida del sistema de información incluyen, por ejemplo, firewalls , servidores de correo electrónico, servidore s web, servidores proxy, servidores de acceso remoto, estaciones de trabajo, equipos portátile s y dispositivos móviles. Los códigos maliciosos incluyen, por ejemplo, virus, gusanos, troyanos y spyware. El código malicioso también puede codificarse en varios formatos (por ejemplo, UUENCODE o Unicode), incluirse en archivos comprimidos u ocultos y ocultarse en archivos mediante esteganografía. El código malicioso se puede transport ar por diferentes medios, como, por ejemplo, accesos		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	a la web, correo electrónico, archivos adjuntos de correo electrónico y dispositi vos de almacenam iento portátiles. Las inserciones de código malicioso se producen mediante la explotaci ón de las vulnerabi lidades del sistema de información. Los mecanismos de protección contra códigos maliciosos incluyen, por ejemplo, las definiciones de firmas antivirus y las tecnologí as basadas en la reputación. Existen diversas tecnologí as y métodos para limitar o eliminar los efectos de los códigos maliciosos. La gestión generalizada de la configuración y los controles exhaustiv os de integridad del software pueden ser eficaces para impedir la ejecución de código no autorizad		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	o. Además del off-the-shelf software comercial, también es posible que haya códigos malicioso s en el software creado a medida. Esto podría incluir, por ejemplo, bombas lógicas, puertas traseras y otros tipos de ciberataques que podrían afectar a las funciones de la organización missions/business . Los mecanismo s tradicionales de protección contra códigos maliciosos no siempre detectan dicho código. En estas situaciones, las organizaciones se basan más bien en otras medidas de seguridad, como las prácticas de codificación seguras, la gestión y el control de la configuración, los procesos de compra de confianza y las prácticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de monitoreo, para garantizar que el software no desempeñe funciones distintas de las previstas. Las organizaciones pueden determinar que, en respuesta a la detección de código malicioso, se puedan garantizar diferente s acciones. Por ejemplo, las organizac iones pueden definir acciones en respuesta a la detección de códigos maliciosos durante los análisis periódicos, acciones en respuesta a la detección de descargas maliciosa s o and/or acciones en respuesta a la detección de código malicioso al intentar abrir o ejecutar archivos. Controles relacionados: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2,		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	SI-4 y SI-7. Referencias: Publicación especial 800-83 del NIST.		
SI-4(1)	La organización conecta y configura las herramientas individuales de detección de intrusos en un sistema de detección de intrusos que abarca todo el sistema de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente de forma continua para detectar actividades o condiciones inusuales o no autorizadas.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente de forma continua para detectar actividades o condiciones inusuales o no autorizadas.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente de forma continua para detectar actividades o condiciones inusuales o no autorizadas.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente de forma continua para detectar actividades o condiciones inusuales o no autorizadas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	cloud-trail-cloud-watch-registros activados	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-5	La organización: a. Recibe alertas, avisos y políticas de seguridad del sistema de información de [asignación: organizaciones externas definidas por la organización] de forma continua; b. Genera alertas, avisos y políticas de seguridad internas según se considere necesario; c. Difunde alertas, avisos y políticas de seguridad entre: [seleccionar (una o más): [asignación: el personal o los roles definidos por la organización]; [asignación: los elementos definidos por la organización dentro de la organización]; [asignación: las organizaciones externas definidas por la organización]]; y d. Implementa las políticas de seguridad de acuerdo con los	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	plazos establecidos o notifica a la organizac ión emisora el grado de incumplimiento. Directriz complemen taria: el equipo de respuesta ante emergencias informáti cas de los Estados Unidos (US-CERT, por sus siglas en inglés) genera alertas y avisos de seguridad para mantener al gobierno federal al corriente de la situación. La Oficina de Administración y Presupuestos de Estados Unidos (OMB, por sus siglas en inglés) u otras organizaciones con la autoridad y responsab ilidad correspon dientes publican las políticas de seguridad . El cumplimiento de las directivas de seguridad es esencial debido a la naturalez a crítica de muchas de estas políticas y a los posibles efectos		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	adversos inmediatos en las operaciones y los activos de la organización, las personas, otras organizaciones y el país si las políticas no se implementan de manera oportuna. Las organizaciones externas incluyen, por ejemplo, mission/business socios externos, socios de la cadena de suministro, proveedores de servicios externos y otras peer/supporting organizaciones. Control relacionado: SI-2. Referencias: Publicación especial 800-40 del NIST.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-5	La organización: a. Recibe alertas, avisos y políticas de seguridad del sistema de informaci ón de [asignaci ón: organizaciones externas definidas por la organización] de forma continua; b. Genera alertas, avisos y políticas de seguridad internas según se considere necesario; c. Difunde alertas, avisos y políticas de seguridad entre: [seleccionar (una o más): [asignaci ón: el personal o los roles definidos por la organizac ión]; [asignación: los elementos definidos por la organización dentro de la organizac ión]; [asignación: las organizaciones externas definidas por la organización]]; y d. Implementa las políticas de seguridad de acuerdo con los	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	plazos establecidos o notifica a la organizac ión emisora el grado de incumplimiento. Directriz complemen taria: el equipo de respuesta ante emergencias informáti cas de los Estados Unidos (US-CERT, por sus siglas en inglés) genera alertas y avisos de seguridad para mantener al gobierno federal al corriente de la situación. La Oficina de Administración y Presupuestos de Estados Unidos (OMB, por sus siglas en inglés) u otras organizaciones con la autoridad y responsab ilidad correspon dientes publican las políticas de seguridad . El cumplimiento de las directivas de seguridad es esencial debido a la naturalez a crítica de muchas de estas políticas y a los posibles efectos		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	adversos inmediatos en las operaciones y los activos de la organización, las personas, otras organizaciones y el país si las políticas no se implementan de manera oportuna. Las organizaciones externas incluyen, por ejemplo, mission/business socios externos, socios de la cadena de suministro, proveedores de servicios externos y otras peer/supporting organizaciones. Control relacionado: SI-2. Referencias: Publicación especial 800-40 del NIST.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-5	La organización: a. Recibe alertas, avisos y políticas de seguridad del sistema de información de [asignación: organizaciones externas definidas por la organización] de forma continua; b. Genera alertas, avisos y políticas de seguridad internas según se considere necesario; c. Difunde alertas, avisos y políticas de seguridad entre: [seleccionar (una o más): [asignación: el personal o los roles definidos por la organización]; [asignación: los elementos definidos por la organización dentro de la organización]; [asignación: las organizaciones externas definidas por la organización]]; y d. Implementa las políticas de seguridad de acuerdo con los	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	plazos establecidos o notifica a la organizac ión emisora el grado de incumplimiento. Directriz complemen taria: el equipo de respuesta ante emergencias informáti cas de los Estados Unidos (US-CERT, por sus siglas en inglés) genera alertas y avisos de seguridad para mantener al gobierno federal al corriente de la situación. La Oficina de Administración y Presupuestos de Estados Unidos (OMB, por sus siglas en inglés) u otras organizaciones con la autoridad y responsab ilidad correspon dientes publican las políticas de seguridad . El cumplimiento de las directivas de seguridad es esencial debido a la naturalez a crítica de muchas de estas políticas y a los posibles efectos		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	adversos inmediatos en las operaciones y los activos de la organización, las personas, otras organizaciones y el país si las políticas no se implementan de manera oportuna. Las organizaciones externas incluyen, por ejemplo, mission/business socios externos, socios de la cadena de suministro, proveedores de servicios externos y otras peer/supporting organizaciones. Control relacionado: SI-2. Referencias: Publicación especial 800-40 del NIST.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-5	La organización: a. Recibe alertas, avisos y políticas de seguridad del sistema de informaci ón de [asignaci ón: organizaciones externas definidas por la organización] de forma continua; b. Genera alertas, avisos y políticas de seguridad internas según se considere necesario; c. Difunde alertas, avisos y políticas de seguridad entre: [seleccionar (una o más): [asignaci ón: el personal o los roles definidos por la organizac ión]; [asignación: los elementos definidos por la organización dentro de la organizac ión]; [asignación: las organizaciones externas definidas por la organización]]; y d. Implementa las políticas de seguridad de acuerdo con los	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	plazos establecidos o notifica a la organizac ión emisora el grado de incumplimiento. Directriz complemen taria: el equipo de respuesta ante emergencias informáti cas de los Estados Unidos (US-CERT, por sus siglas en inglés) genera alertas y avisos de seguridad para mantener al gobierno federal al corriente de la situación. La Oficina de Administración y Presupuestos de Estados Unidos (OMB, por sus siglas en inglés) u otras organizaciones con la autoridad y responsab ilidad correspon dientes publican las políticas de seguridad . El cumplimiento de las directivas de seguridad es esencial debido a la naturalez a crítica de muchas de estas políticas y a los posibles efectos		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	adversos inmediatos en las operaciones y los activos de la organización, las personas, otras organizaciones y el país si las políticas no se implementan de manera oportuna. Las organizaciones externas incluyen, por ejemplo, mission/business socios externos, socios de la cadena de suministro, proveedores de servicios externos y otras peer/supporting organizaciones. Control relacionado: SI-2. Referencias: Publicación especial 800-40 del NIST.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(1)	El sistema de información comprueba la integridad de los eventos relevante s para la seguridad al menos una vez al mes.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(1)	El sistema de información comprueba la integridad de los eventos relevante s para la seguridad al menos una vez al mes.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(1)	El sistema de información comprueba la integridad de los eventos relevantes para la seguridad al menos una vez al mes.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7	La organización emplea herramientas de verificación de la integridad para detectar cambios no autorizados en [asignación: software, firmware e información definidos por la organización].	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcionan la información necesaria para las acciones correctivas sin revelar información que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignación: al personal o los roles definidos por la organización]. Guía complementaria: Organizations considera detenidamente los mensajes structure/content de error. La medida en que los sistemas de información son capaces de identificar y gestionar las condiciones de error depende de la política de la organización y los requisitos operativos. La información que	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	podrían aprovecha r los adversarios incluye, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como nombre de usuario, la mission/b usiness información que puede derivarse de la información registrada (si no se indica explícita mente) y la informaci ón personal, como números de cuenta, números de seguro social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcio nan la información necesaria para las acciones correctivas sin revelar informaci ón que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignaci ón: al personal o los roles definidos por la organización]. Guía complemen taria: Organizations considera detenidam ente los mensajes structure/content de error. La medida en que los sistemas de información son capaces de identific ar y gestionar las condiciones de error depende de la política de la organizac ión y los requisito s operativos. La información que	cloud-trail-cloud-watch-Habilitado para los registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	podrían aprovecha r los adversarios incluye, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como nombre de usuario, la mission/b usiness información que puede derivarse de la información registrada (si no se indica explícita mente) y la informaci ón personal, como números de cuenta, números de seguro social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcio nan la información necesaria para las acciones correctivas sin revelar informaci ón que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignaci ón: al personal o los roles definidos por la organización]. Guía complemen taria: Organizations considera detenidam ente los mensajes structure/content de error. La medida en que los sistemas de información son capaces de identific ar y gestionar las condiciones de error depende de la política de la organizac ión y los requisito s operativos. La información que	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilaci ón se envíen a Amazon CloudWatc h o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	podrían aprovecha r los adversarios incluye, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como nombre de usuario, la mission/b usiness información que puede derivarse de la información registrada (si no se indica explícita mente) y la informaci ón personal, como números de cuenta, números de seguro social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcionan la información necesaria para las acciones correctivas sin revelar información que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignación: al personal o los roles definidos por la organización]. Guía complementaria: Organizations considera detenidamente los mensajes structure/content de error. La medida en que los sistemas de información son capaces de identificar y gestionar las condiciones de error depende de la política de la organización y los requisitos operativos. La información que	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	podrían aprovecha r los adversarios incluye, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como nombre de usuario, la mission/b usiness información que puede derivarse de la información registrada (si no se indica explícita mente) y la informaci ón personal, como números de cuenta, números de seguro social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcio nan la información necesaria para las acciones correctivas sin revelar informaci ón que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignaci ón: al personal o los roles definidos por la organización]. Guía complemen taria: Organizations considera detenidam ente los mensajes structure/content de error. La medida en que los sistemas de información son capaces de identific ar y gestionar las condiciones de error depende de la política de la organizac ión y los requisito s operativos. La información que	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	podrían aprovecha r los adversarios incluye, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como nombre de usuario, la mission/b usiness información que puede derivarse de la información registrada (si no se indica explícita mente) y la informaci ón personal, como números de cuenta, números de seguro social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcio nan la información necesaria para las acciones correctivas sin revelar informaci ón que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignaci ón: al personal o los roles definidos por la organización]. Guía complemen taria: Organizations considera detenidam ente los mensajes structure/content de error. La medida en que los sistemas de información son capaces de identific ar y gestionar las condiciones de error depende de la política de la organizac ión y los requisito s operativos. La información que	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	podrían aprovecha r los adversarios incluye, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como nombre de usuario, la mission/b usiness información que puede derivarse de la información registrada (si no se indica explícita mente) y la informaci ón personal, como números de cuenta, números de seguro social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcio nan la información necesaria para las acciones correctivas sin revelar informaci ón que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignaci ón: al personal o los roles definidos por la organización]. Guía complemen taria: Organizations considera detenidam ente los mensajes structure/content de error. La medida en que los sistemas de información son capaces de identific ar y gestionar las condiciones de error depende de la política de la organizac ión y los requisito s operativos. La información que	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y transmitidos a Amazon CloudWatc h Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditoría s de seguridad y acceso, y pueden ayudar a diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	podrían aprovecha r los adversarios incluye, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como nombre de usuario, la mission/b usiness información que puede derivarse de la información registrada (si no se indica explícita mente) y la informaci ón personal, como números de cuenta, números de seguro social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	dynamodb-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	rds-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-16	El sistema de información implementa [asignación: medidas de seguridad definidas por la organización] para proteger su memoria de la ejecución no autorizada de código. Directriz complementaria: algunos adversarios lanzan ataques con la intención de ejecutar código en regiones de memoria no ejecutables o en ubicaciones de memoria prohibidas. Las medidas de seguridad empleadas para proteger la memoria incluyen, por ejemplo, la prevención de la ejecución de datos y la asignación al azar del diseño del espacio de las direcciones. Las medidas de prevención de la ejecución de datos se pueden aplicar mediante	ecs-task-definition-memory-límite estricto	Limitar el máximo de memoria disponible para los contenedores de Amazon Elastic Container Service (ECS) garantiza que no se haga un uso indebido de los recursos en caso de que se produzca un acceso malintencionado a los contenedores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	hardware o software. El hardware proporcio na la mayor solidez del mecanismo. Controles relaciona dos: AC-25 y SC-3. Mejoras del control: ninguna. Referencias: ninguna.		

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para FedRAMP (moderada).

Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 1)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear comprobaciones de control de seguridad, operativas o de optimización de costos mediante reglas de AWS Config administradas o personalizadas y acciones correctivas de AWS Config. Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación se proporciona un ejemplo de asignación entre el Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP, por sus siglas en inglés) y las reglas de AWS Config administradas. Cada regla de Config se aplica a un recurso de AWS específico que está relacionado con uno o más controles del FedRAMP. Un control del FedRAMP puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector , Amazon Macie, AWS Identity and Access Managemen t (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas

ID de control	Descripción del control	Regla de AWS Config	Directrices
			incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicación de DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	elasticsearch-in-vpc-only	Gestione el acceso a la nube de AWS de manera que se garantice que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h Service dentro de una Amazon VPC garantiza una comunicación segura entre OpenSearc h Service y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de Internet, un dispositivo NAT o una conexión de VPN.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	ec-2 instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Amazon VPC para gestionar correctamente el acceso.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	Regla de AWS Config	Directrices
			deben asignarse a una VPC.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterm inado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la nube de AWS de manera que garantice que no se asigne automáticamente una dirección IP pública a las subredes de Amazon Virtual Private Cloud (VPC). Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	alb-http-to-https-comprobación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida y compruebe que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (Valor de las prácticas recomendadas de seguridad básica de AWS: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	elb-acm-certificate-required	RELLENAR ESTO
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomiend a que se utilicen políticas administr adas en lugar de políticas insertadas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios de IAM, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(12)(a)	La organización: a. Monitorea las cuentas del sistema de información para detectar [asignación: un uso atípico definido por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(12)(a)	La organización: a. Monitorea las cuentas del sistema de información para detectar [asignación: un uso atípico definido por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(3)	El sistema de información desactiva automáticamente las cuentas de usuario inactivas tras 90 días.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(3)	El sistema de información desactiva automáticamente las cuentas de usuario inactivas tras 90 días.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireLowercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireSy mbols (valor de Prácticas recomenda das de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administr ar de forma centraliz ada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada que permita acciones bloqueadas en todas las claves de AWS Key Management Service. AWS recomienda que utilice políticas administradas en lugar de políticas insertadas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el parámetro blockedActionsPatterns. (Valor de las prácticas recomendadas de seguridad básica de AWS: kms:Decrypt,

ID de control	Descripción del control	Regla de AWS Config	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomiend a que se utilicen políticas administradas en lugar de políticas insertadas. Las políticas administradas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios de IAM, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector , Amazon Macie, AWS Identity and Access Managemen t (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administr ar de forma centraliz ada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de información.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de información.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y que se transmita n a los registros de Amazon CloudWatc h para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireLowercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireSy mbols (valor de Prácticas recomenda das de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcional idad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y separación de funciones con permisos y autorizaciones de acceso, ya que garantiza que los grupos de IAM tengan al menos un usuario de IAM. Una forma de incorporar el privilegio mínimo es colocar a los usuarios de IAM en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, lo que impide que las políticas incluyan acciones bloqueadas en todas las claves del AWS Key Management Service. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el parámetro blockedActionsPatterns. (Valor de las prácticas recomendadas de seguridad básica de AWS: kms:Decrypt, kms:ReEncryptFrom). Los valores reales deben reflejar las

ID de control	Descripción del control	Regla de AWS Config	Directrices
			políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada que permita acciones bloqueada s en todas las claves de AWS Key Management Service. AWS recomienda que utilice políticas administradas en lugar de políticas insertadas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el parámetro blockedActionsPatt erns. (Valor de las prácticas recomenda das de seguridad básica de AWS: kms:Decrypt,

ID de control	Descripción del control	Regla de AWS Config	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomiend a que se utilicen políticas administr adas en lugar de políticas insertadas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protecció n además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios de IAM, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	ec-2 instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.
AC-21(b)	La organización: b. Emplea [asignaci ón: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicación de DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a internet para las cargas de trabajo dentro de las Amazon VPC puede reducir el acceso no deseado a su entorno.
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la nube de AWS de manera que garantice que no se asigne automáticamente una dirección IP pública a las subredes de Amazon Virtual Private Cloud (VPC). Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-21(b)	La organización: b. Emplea [asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre el intercambio de información o la colaboración.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterminado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcional idad mínima.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicaci ón de DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y separación de funciones con permisos y autorizaciones de acceso, ya que garantiza que los grupos de IAM tengan al menos un usuario de IAM. Una forma de incorporar el privilegio mínimo es colocar a los usuarios de IAM en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El método IMDSv2 utiliza controles basados en sesiones. IMDSv2 permite implementar controles para restringir los cambios en los metadatos de la instancia.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ec-2 instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomiend a que se utilicen políticas administr adas en lugar de políticas insertadas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	elasticsearch-in-vpc-only	Gestione el acceso a la nube de AWS de manera que se garantice que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h Service dentro de una Amazon VPC garantiza una comunicación segura entre OpenSearc h Service y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de Internet, un dispositivo NAT o una conexión de VPN.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	Regla de AWS Config	Directrices
			deben asignarse a una VPC.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterm inado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la nube de AWS de manera que garantice que no se asigne automáticamente una dirección IP pública a las subredes de Amazon Virtual Private Cloud (VPC). Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	Regla de AWS Config	Directrices
			deben asignarse a una VPC.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	ec-2 instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidenc ialidad de los sistemas. Esta regla le permite configura r de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,338 9,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizad os acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida y compruebe que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (Valor de las prácticas recomendadas de seguridad básica de AWS: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	elasticsearch-in-vpc-only	Gestione el acceso a la nube de AWS de manera que se garantice que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h Service dentro de una Amazon VPC garantiza una comunicación segura entre OpenSearc h Service y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de Internet, un dispositivo NAT o una conexión de VPN.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicación de DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y separación de funciones con permisos y autorizaciones de acceso, ya que garantiza que los grupos de IAM tengan al menos un usuario de IAM. Una forma de incorporar el privilegio mínimo es colocar a los usuarios de IAM en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, lo que impide que las políticas incluyan acciones bloqueadas en todas las claves del AWS Key Management Service. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el parámetro blockedActionsPatterns. (Valor de las prácticas recomendadas de seguridad básica de AWS: kms:Decrypt, kms:ReEncryptFrom) . Los valores reales deben reflejar las

ID de control	Descripción del control	Regla de AWS Config	Directrices
			políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada que permita acciones bloqueadas en todas las claves de AWS Key Management Service. AWS recomienda que utilice políticas administradas en lugar de políticas insertadas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el parámetro blockedActionsPatterns. (Valor de las prácticas recomendadas de seguridad básica de AWS: kms:Decrypt,

ID de control	Descripción del control	Regla de AWS Config	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomiend a que se utilicen políticas administradas en lugar de políticas insertadas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales de autenticación AWS_ACCESS_KEY_ID y AWS_SECRET_ACCESS_KEY no existan en los entornos de proyecto de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y separación de funciones con permisos y autorizaciones de acceso, ya que garantiza que los grupos de IAM tengan al menos un usuario de IAM. Una forma de incorporar el privilegio mínimo es colocar a los usuarios de IAM en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicación de DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El método IMDSv2 utiliza controles basados en sesiones. IMDSv2 permite implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomiend a que se utilicen políticas administradas en lugar de políticas insertadas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	elasticsearch-in-vpc-only	Gestione el acceso a la nube de AWS de manera que se garantice que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch Service dentro de una Amazon VPC garantiza una comunicación segura entre OpenSearch Service y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de Internet, un dispositivo NAT o una conexión de VPN.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ec-2 instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Amazon VPC para gestionar correctamente el acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	Regla de AWS Config	Directrices
			deben asignarse a una VPC.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterminado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la nube de AWS de manera que garantice que no se asigne automáticamente una dirección IP pública a las subredes de Amazon Virtual Private Cloud (VPC). Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
AC-6(2)	El sistema de información exige el uso de cuentas sin privilegios cuando se accede a funciones que no son de seguridad y limita la exposición al operar desde cuentas o roles con privilegios	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(2)	El sistema de información exige el uso de cuentas sin privilegios cuando se accede a funciones que no son de seguridad y limita la exposición al operar desde cuentas o roles con privilegios	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(2)	El sistema de información exige el uso de cuentas sin privilegios cuando se accede a funciones que no son de seguridad y limita la exposición al operar desde cuentas o roles con privilegios	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcional idad mínima.
AC-6(9)	El sistema de información registra la ejecución de funciones con privilegi os.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administr ar de forma centraliz ada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(9)	El sistema de información registra la ejecución de funciones con privilegios.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(9)	El sistema de información registra la ejecución de funciones con privilegios.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AC-6(9)	El sistema de información registra la ejecución de funciones con privilegios.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y que se transmitan a los registros de Amazon CloudWatch para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(9)	El sistema de información registra la ejecución de funciones con privilegios.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
AC-6(9)	El sistema de información registra la ejecución de funciones con privilegios.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(9)	El sistema de información registra la ejecución de funciones con privilegios.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(9)	El sistema de información registra la ejecución de funciones con privilegios.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(10)	El sistema de información impide que los usuarios sin privilegios ejecuten funciones con privilegios, como deshabilitar, eludir o alterar las protecciones o contramedidas de seguridad implementadas.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(10)	El sistema de información impide que los usuarios sin privilegios ejecuten funciones con privilegios, como deshabilitar, eludir o alterar las protecciones o contramedidas de seguridad implementadas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6(10)	El sistema de información impide que los usuarios sin privilegios ejecuten funciones con privilegios, como deshabilitar, eludir o alterar las protecciones o contramedidas de seguridad implementadas.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AU-11	La organización conserva los registros de auditoría durante al menos 90 días para respaldar las investigaciones posteriores de los incidentes de seguridad y cumplir con los requisitos reglamentarios y organizativos de conservación de la información.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	api-gw-execution-l ogging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administr ar de forma centraliz ada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	wafv2-logging-enab led	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimiento de procesos y eventos del sistema. Para las aplicaciones web: toda la actividad del administrador, las comprobaciones de autenticación, las comprobaciones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditables definidos en el AU-2 a. deberá auditarse continuamente para cada evento identificado].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administr ar de forma centraliz ada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditables definidos en el AU-2 a. deberá auditarse continuamente para cada evento identificado].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimiento de procesos y eventos del sistema. Para las aplicaciones web: toda la actividad del administrador, las comprobaciones de autenticación, las comprobaciones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditables definidos en el AU-2 a. deberá auditarse continuamente para cada evento identificado].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditables definidos en el AU-2 a. deberá auditarse continuamente para cada evento identificado].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditables definidos en el AU-2 a. deberá auditarse continuamente para cada evento identificado].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		necesidad de realizar ninguna acción.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditables definidos en el AU-2 a. deberá auditarse continuamente para cada evento identificado].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditables definidos en el AU-2 a. deberá auditarse continuamente para cada evento identificado].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditables definidos en el AU-2 a. deberá auditarse continuamente para cada evento identificado].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimiento de procesos y eventos del sistema. Para las aplicaciones web: toda la actividad del administrador, las comprobaciones de autenticación, las comprobaciones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimiento de procesos y eventos del sistema. Para las aplicaciones web: toda la actividad del administrador, las comprobaciones de autenticación, las comprobaciones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditables definidos en el AU-2 a. deberá auditarse continuamente para cada evento identificado].		
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaci ona los registros de auditoría en diferente s repositorios para conocer la situación en toda la organizac ión.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y que se transmita n a los registros de Amazon CloudWatc h para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaci ona los registros de auditoría en diferente s repositorios para conocer la situación en toda la organizac ión.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AU-6(3)	La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-6(3)	La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaci ona los registros de auditoría en diferente s repositorios para conocer la situación en toda la organizac ión.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaci ona los registros de auditoría en diferente s repositorios para conocer la situación en toda la organizac ión.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaci ona los registros de auditoría en diferente s repositorios para conocer la situación en toda la organizac ión.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaci ona los registros de auditoría en diferente s repositorios para conocer la situación en toda la organizac ión.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaci ona los registros de auditoría en diferente s repositorios para conocer la situación en toda la organizac ión.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaci ona los registros de auditoría en diferente s repositorios para conocer la situación en toda la organizac ión.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(3)	La organización analiza y correlaci ona los registros de auditoría en diferente s repositorios para conocer la situación en toda la organizac ión.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-7	El sistema de información proporcio na e implement a una capacidad de reducción de registros de auditoría y generación de informes. Dicha capacidad (a) ofrece soporte para los requisitos de revisión, análisis y generació n de informes de los registros de auditoría bajo demanda, así como para la investigación posterior al incidente; y (b) no altera el contenido original ni el orden temporal de los registros de auditoría.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administr ar de forma centraliz ada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-7	El sistema de información proporcio na e implement a una capacidad de reducción de registros de auditoría y generación de informes. Dicha capacidad (a) ofrece soporte para los requisitos de revisión, análisis y generació n de informes de los registros de auditoría bajo demanda, así como para la investigación posterior al incidente; y (b) no altera el contenido original ni el orden temporal de los registros de auditoría.	cloud-trail-log-fi le-habilitada para validación	Utilice la validació n de los archivos de registro de AWS CloudTrail para comprobar la integrida d de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar , eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-7(1)	El sistema de información permite procesar los registros de auditoría de eventos de interés en función de [asignación: campos de auditoría definidos por la organización dentro de los registros de auditoría].	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-7(1)	El sistema de información permite procesar los registros de auditoría de eventos de interés en función de [asignación: campos de auditoría definidos por la organización dentro de los registros de auditoría].	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.
AU-9	El sistema de información protege la información de auditoría y las herramientas de auditoría contra todo acceso, modificación y eliminación no autorizados.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
AU-9	El sistema de información protege la información de auditoría y las herramientas de auditoría contra todo acceso, modificación y eliminación no autorizados.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-9	El sistema de información protege la información de auditoría y las herramientas de auditoría contra todo acceso, modificación y eliminación no autorizados.	cloud-trail-log-file-habilitada para validación	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-9(2)	El sistema de información hace copias de seguridad de los registros de auditoría al menos una vez por semana en un sistema o componente del sistema físicamente diferente del sistema o componente que se está auditando.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-9(2)	El sistema de información hace copias de seguridad de los registros de auditoría al menos una vez por semana en un sistema o componente del sistema físicamente diferente del sistema o componente que se está auditando.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y que se transmita n a los registros de Amazon CloudWatc h para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AU-12	El sistema de información proporciona la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organización]; (b) permite que [asignación: personal o roles definidos por la organización] seleccionen los tipos de eventos que van a ser registrados por componentes específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	api-gw-execution-l ogging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administr ar de forma centraliz ada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	El sistema de información proporcio na la capacidad de generar registros de auditoría para los tipos de eventos que el sistema puede auditar, según se define en AU-2a, en los [asignación: componentes del sistema definidos por la organizac ión]; (b) permite que [asignación: personal o roles definidos por la organizac ión] seleccionen los tipos de eventos que van a ser registrad os por component es específicos del sistema; y (c) genera registros de auditoría para los tipos de eventos definidos en AU-2c que incluyen el contenido del registro de auditoría definido en AU-3.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorear; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	ec-2 instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorear; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorear; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorear; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	beanstalk-enhanced-health-reporting-habilitado	Los informes de estado mejorados de AWS Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcio nan un descriptor de estado para evaluar la gravedad de los problemas detectado s e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	dynamodb-throughpu t-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisio nada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de actividad de lectura y escritura que puede admitir cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficient es para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configura r de forma opcional los parámetros accountRCUThreshol dPercentage (valor predeterminado de Config: 80) y accountWCUThreshol dPercentage (valor

ID de control	Descripción del control	Regla de AWS Config	Directrices
			predeterminado de Config: 80). Los valores reales deben reflejar las políticas de su organización.
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultane idad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administr ación de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	ec2- -comprobar managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec-2 volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidenc ialidad de los sistemas. Esta regla le permite configura r de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,338 9,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicacio nes web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicación de DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	elasticsearch-in-vpc-only	Gestione el acceso a la nube de AWS de manera que se garantice que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h Service dentro de una Amazon VPC garantiza una comunicación segura entre OpenSearc h Service y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de Internet, un dispositivo NAT o una conexión de VPN.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	ec-2 instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Amazon VPC para gestionar correctamente el acceso.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	Regla de AWS Config	Directrices
			deben asignarse a una VPC.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a internet para las cargas de trabajo dentro de las Amazon VPC puede reducir el acceso no deseado a su entorno.
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	s3- bucket-level-publi c-access -prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la nube de AWS de manera que garantice que no se asigne automáticamente una dirección IP pública a las subredes de Amazon Virtual Private Cloud (VPC). Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	autoscaling-launch -config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	api-gw-associated-with-guerra	AWS WAF permite configurar un conjunto de reglas (denomina das lista de control de acceso web (ACL web) que permiten, bloquean o cuentan solicitudes web en función de las reglas y condicion es de seguridad web personalizables que defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterminado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
CM-7(a)	La organización: a. Configura el sistema de información para proporcionar solo las capacidades esenciales.	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-7(a)	La organización: a. Configura el sistema de información para proporcionar solo las capacidades esenciales.	ec2- -comprobar managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-7(a)	La organización: a. Configura el sistema de información para proporcionar solo las capacidades esenciales.	ec-2 instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-8(1)	La organización actualiza el inventario de los componentes del sistema de información como parte integral de las instalaciones de componentes, desmontajes y actualizaciones del sistema de información.	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-8(1)	La organización actualiza el inventario de los componentes del sistema de información como parte integral de las instalaciones de componentes, desmontajes y actualizaciones del sistema de información.	ec2- -comprobar managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados de forma continua, con un retraso máximo de cinco minutos en la detección, para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información.	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados de forma continua, con un retraso máximo de cinco minutos en la detección, para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información.	ec2- -comprobar managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados de forma continua, con un retraso máximo de cinco minutos en la detección, para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información.	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados de forma continua, con un retraso máximo de cinco minutos en la detección, para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-6 (1)	La organización identifica un sitio de almacenamiento alternativo que esté lo suficientemente separado del sitio de almacenamiento principal como para reducir la susceptib ilidad a las mismas amenazas.	dynamodb-in-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus tablas de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-6 (1)	La organización identifica un sitio de almacenamiento alternativo que esté lo suficientemente separado del sitio de almacenamiento principal como para reducir la susceptib ilidad a las mismas amenazas.	ebs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-6 (1)	La organización identifica un sitio de almacenamiento alternativo que esté lo suficientemente separado del sitio de almacenamiento principal como para reducir la susceptib ilidad a las mismas amenazas.	efs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administr ado con una solución de copia de seguridad basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-6 (1)	La organización identifica un sitio de almacenamiento alternativo que esté lo suficientemente separado del sitio de almacenamiento principal como para reducir la susceptibilidad a las mismas amenazas.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-6 (1)	La organización identifica un sitio de almacenamiento alternativo que esté lo suficientemente separado del sitio de almacenamiento principal como para reducir la susceptibilidad a las mismas amenazas.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-6 (1)	La organización identifica un sitio de almacenamiento alternativo que esté lo suficientemente separado del sitio de almacenamiento principal como para reducir la susceptibilidad a las mismas amenazas.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando se habilitan las copias de seguridad automáticas, Amazon ElastiCache crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-6 (1)	La organización identifica un sitio de almacenamiento alternativo que esté lo suficientemente separado del sitio de almacenamiento principal como para reducir la susceptibilidad a las mismas amenazas.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-6 (1)	La organización identifica un sitio de almacenamiento alternativo que esté lo suficientemente separado del sitio de almacenamiento principal como para reducir la susceptibilidad a las mismas amenazas.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuenci a definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documenta ción relacionada	dynamodb-in-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus tablas de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuenci a definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documenta ción relacionada	ebs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuenci a definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documenta ción relacionada	efs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administr ado con una solución de copia de seguridad basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documentación relacionada	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuenci a definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documenta ción relacionada	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuenci a definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documenta ción relacionada	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documentación relacionada	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documentación relacionada	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional dedicada para las operaciones de E/S de Amazon EBS. Esta optimización ofrece el mejor rendimiento para sus volúmenes de EBS, ya que reduce al mínimo la contención entre las operaciones de E/S de Amazon EBS y otro tráfico procedente de la instancia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuenci a definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documenta ción relacionada	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando se habilitan las copias de seguridad automátic as, Amazon ElastiCac he crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuenci a definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documenta ción relacionada	redshift-cluster-m aintenancesettings-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documentación relacionada	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9	El sistema de información (a) realiza copias de seguridad en el nivel de usuario de la información contenida en los [asignación: componentes del sistema definidos por la organización], con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (b) realiza copias de seguridad de la información en el nivel de sistema contenida en el sistema, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; (c) realiza copias de seguridad de la documentación del sistema, lo que incluye la documentación relacionada	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la seguridad y la privacidad, con la [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación]; y Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB usa el servicio de escalado automático de aplicaciones de AWS para ajustar de manera automática a la capacidad de rendimiento aprovisionada en respuesta a los patrones de tráfico reales. Esto permite a una tabla o índice secundario global incrementar su capacidad de lectura y escritura aprovisionada para gestionar incrementos repentinos del tráfico sin limitaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	Regla de AWS Config	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando se habilitan las copias de seguridad automátic as, Amazon ElastiCac he crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	vpc-vpn-2-tunnels-up	Para cumplir los requisitos de resiliencia, pueden implementarse túneles de Site-to-Site VPN redundantes. Se utilizan dos túneles para garantizar la conectividad en caso de que una de las conexiones de Site-to-Site VPN no esté disponible. Para protegerse frente a la pérdida de conectividad que se produciría si su puerta de enlace de cliente dejara de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN con la Amazon Virtual Private Cloud (Amazon VPC) y la puerta de enlace privada virtual con otro dispositivo de puerta de enlace de cliente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	elb-cross-zone-loa d-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELB) para poder conservar la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional dedicada para las operaciones de E/S de Amazon EBS. Esta optimización ofrece el mejor rendimiento para sus volúmenes de EBS, ya que reduce al mínimo la contención entre las operaciones de E/S de Amazon EBS y otro tráfico procedente de la instancia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de copia de seguridad de datos, asegúrese de que su plan de AWS Backup esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer los parámetros requiredFrequencyValue (valor predeterminado de Config: 1), requiredRetentionDays (valor predeterminado de Config: 35) y

ID de control	Descripción del control	Regla de AWS Config	Directrices
			requiredFrequencyUnit (valor predeterminado de Config: days). El valor real debe reflejar los requisitos de su organización.
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	fsx-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus sistemas de archivos de Amazon FSx formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	ec2-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	aurora-resources-p rotected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	dynamodb-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	ebs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	efs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	rds-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un plan de AWSBackup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando se habilitan las copias de seguridad automátic as, Amazon ElastiCac he crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de copia de seguridad de datos, asegúrese de que su plan de AWS Backup esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer los parámetros requiredFrequencyValue (valor predeterminado de Config: 1), requiredRetentionDays (valor predeterminado de Config: 35) y

ID de control	Descripción del control	Regla de AWS Config	Directrices
			requiredFrequencyUnit (valor predeterminado de Config: days). El valor real debe reflejar los requisitos de su organización.
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	fsx-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus sistemas de archivos de Amazon FSx formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	ec2-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	aurora-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de informaci ón (se increment an diariamen te; completas semanalmente).	dynamodb-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	ebs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	efs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información de nivel de sistema contenida en el sistema de información (se incrementan diariamente; completas semanalmente).	rds-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un plan de AWSBackup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-2	El sistema de información identifica y autentica de forma única a los usuarios de la organización (o los procesos que actúan en nombre de los usuarios de la organización).	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireLowercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireSy mbols (valor de Prácticas recomenda das de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-2	El sistema de información identifica y autentica de forma única a los usuarios de la organización (o los procesos que actúan en nombre de los usuarios de la organización).	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcional idad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-2(1)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-2(1)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios de IAM, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-2(1)(2)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (2) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas sin privilegios.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios de IAM, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-2(1)(2)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (2) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas sin privilegios.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-5(1)(a)(d)(e)	Para la autenticación basada en contraseñas, el sistema de información: a. Aplica una complejidad mínima de las contraseñas con [asignación: requisitos definidos por la organización en cuanto a la distinción entre mayúsculas y minúsculas, números de caracteres, mezcla de letras mayúsculas y letras minúsculas, números y caracteres especiales, incluidos los requisitos mínimos de cada tipo]; d. Aplica las restricciones de duración mínima y máxima de las contraseñas de [asignación: números definidos por la organización para una vida útil mínima y máxima]; e. Prohíbe la reutilización de contraseñas durante 24 generaciones.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-5(4)	La organización emplea herramientas automatizadas para determinar si los autenticadores de contraseñas son lo suficientemente seguros como para cumplir [asignación: los requisitos definidos por la organización].	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-5(7)	La organización se asegura de que los autenticadores estáticos no cifrados no estén integrados en las aplicaciones o los scripts de acceso ni se almacenen en las teclas de función.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales de autenticación AWS_ACCESS_KEY_ID y AWS_SECRET_ACCESS_KEY no existan en los entornos de proyecto de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	guardduty-non-archived-findings	Amazon GuardDuty le ayuda a comprender el efecto de un incidente al clasificar los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional daysLowSev (valor predeterminado de Config: 30), daysMediumSev (valor predeterminado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-6(1)	La organización emplea mecanismos automatizados para ayudar a denunciar los incidentes de seguridad.	guardduty-non-archived-findings	Amazon GuardDuty le ayuda a comprender el efecto de un incidente al clasificar los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional daysLowSev (valor predeterminado de Config: 30), daysMediumSev (valor predeterminado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-6(1)	La organización emplea mecanismos automatizados para ayudar a denunciar los incidentes de seguridad.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-6(1)	La organización emplea mecanismos automatizados para ayudar a denunciar los incidentes de seguridad.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-7(1)	La organización emplea mecanismos automatizados para aumentar la disponibilidad de la información y el apoyo relacionados con la respuesta a los incidentes.	guardduty-non-archived-findings	Amazon GuardDuty le ayuda a comprender el efecto de un incidente al clasificar los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional daysLowSev (valor predeterminado de Config: 30), daysMediumSev (valor predeterminado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-7(1)	La organización emplea mecanismos automatizados para aumentar la disponibilidad de la información y el apoyo relacionados con la respuesta a los incidentes.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-7(1)	La organización emplea mecanismos automatizados para aumentar la disponibilidad de la información y el apoyo relacionados con la respuesta a los incidentes.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-5	La organización: a. Realiza un análisis en busca de vulnerabi lidades en el sistema de información y las aplicaciones alojadas [asignación: frecuencia definida por la organización o de forma aleatoria de acuerdo con un proceso definido por la organizac ión] y cuando se identifican y notifican nuevas vulnerabi lidades que puedan afectar al sistema o las aplicaciones; b. Emplea herramien tas y técnicas de análisis de vulnerabi lidades que facilitan la interoperabilidad entre las herramien tas y automatizan partes del proceso de administración de vulnerabilidades mediante el uso de estándares para: 1. Enumerar las plataformas, los	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	defectos del software y las configura ciones incorrectas; 2. Formatear las listas de verificac ión y los procedimi entos de prueba; y 3. Medir el impacto de la vulnerabi lidad; c. Analiza los informes de análisis de vulnerabilidades y los resultados de las evaluacio nes de control de seguridad; d. Corrige las vulnerabilidades legítimas [asignación: tiempos de respuesta definidos por la organización], de acuerdo con una evaluación organizat iva del riesgo; y e. Comparte la informaci ón obtenida del proceso de análisis de vulnerabilidades y las evaluaciones de control de seguridad con [asignación: personal o roles definidos por la organización] para		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	ayudar a eliminar vulnerabilidades similares en otros sistemas de informaci ón (es decir, debilidad es o deficiencias sistémicas).		

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-5	La organización: a. Realiza análisis mensuales en busca de vulnerabilidades en el sistema de información y las aplicaciones alojadas [sistema operativo /infraestructura; aplicaciones web y bases de datos mensualmente] y cuando se identifican y notifican nuevas vulnerabilidades que puedan afectar al sistema o las aplicaciones; b. Emplea herramientas y técnicas de análisis de vulnerabilidades que facilitan la interoperabilidad entre las herramientas y automatizan partes del proceso de administración de vulnerabilidades mediante el uso de estándares para: 1. Enumerar las plataformas, los defectos del software	guardduty-non-archived-findings	Amazon GuardDuty le ayuda a comprender el efecto de un incidente al clasificar los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional daysLowSev (valor predeterminado de Config: 30), daysMediumSev (valor predeterminado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	y las configura ciones incorrectas; 2. Formatear las listas de verificac ión y los procedimi entos de prueba; y 3. Medir el impacto de la vulnerabi lidad; c. Analiza los informes de análisis de vulnerabilidades y los resultados de las evaluacio nes de control de seguridad; d. Corrige las vulnerabi lidades legítimas: las vulnerabilidades de alto riesgo se mitigan en un plazo de treinta (30) días a partir de la fecha de su descubrimiento; las vulnerabilidades de riesgo moderado se mitigan en un plazo de noventa (90) días a partir de la fecha de su descubrimiento; las vulnerabilidades de bajo riesgo se mitigan en un plazo de ciento ochenta (180) días a partir de la fecha de		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	su descubrimiento, de acuerdo con una evaluación organizativa del riesgo; y e. Comparte la información obtenida del proceso de análisis de vulnerabilidades y las evaluaciones de control de seguridad con [asignación: personal o roles definidos por la organización] para ayudar a eliminar vulnerabilidades similares en otros sistemas de información (es decir, debilidades o deficiencias sistémicas).		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-10	La organización exige al desarrollador del sistema de informaci ón, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el desarrollo, la implementación y el funcionamiento del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d. Documente los cambios aprobados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-10	La organización exige al desarrollador del sistema de información, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el desarrollo, la implementación y el funcionamiento del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d. Documente los cambios aprobados	guardduty-non-arch ived-findings	Amazon GuardDuty le ayuda a comprende r el efecto de un incidente al clasifica r los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridad es de corrección. Esta regla le permite configurar de forma opcional daysLowSe v (valor predeterm inado de Config: 30), daysMediumSev (valor predeterm inado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-10	La organización exige al desarrollador del sistema de informaci ón, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el desarrollo, la implementación y el funcionamiento del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d. Documente los cambios aprobados	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector , Amazon Macie, AWS Identity and Access Managemen t (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-10	La organización exige al desarrollador del sistema de informaci ón, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el desarrollo, la implementación y el funcionamiento del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d. Documente los cambios aprobados	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administr ación de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-3(a)	La organización: a. Administra el sistema de información mediante [asignación: el ciclo de vida de desarrollo del sistema definido por la organización] que incorpora consideraciones de seguridad de la información.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales de autenticación AWS_ACCESS_KEY_ID y AWS_SECRET_ACCESS_KEY no existan en los entornos de proyecto de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-3(a)	La organización: a. Administra el sistema de información mediante [asignación: el ciclo de vida de desarrollo del sistema definido por la organización] que incorpora consideraciones de seguridad de la información.	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-3(a)	La organización: a. Administra el sistema de información mediante [asignación: el ciclo de vida de desarrollo del sistema definido por la organización] que incorpora consideraciones de seguridad de la información.	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio de origen de GitHub o Bitbucket no contenga tokens de acceso personal, nombres de usuario ni contraseñas en los entornos de proyectos de AWS Codebuild. En lugar de tokens de acceso personal o un nombre de usuario y contraseña, utilice OAuth a fin de conceder autorización para el acceso a repositorios de GitHub o Bitbucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-12	La organización establece y administra las claves criptográficas para la criptografía requerida empleada en el sistema de información de acuerdo con [asignación: requisitos definidos por la organización para la generación, distribución, almacenamiento, acceso y destrucción de claves].	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-12	La organización establece y administra las claves criptográficas para la criptografía requerida empleada en el sistema de información de acuerdo con [asignación: requisitos definidos por la organización para la generación, distribución, almacenamiento, acceso y destrucción de claves].	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida y compruebe que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (Valor de las prácticas recomendadas de seguridad básica de AWS: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-12	La organización establece y administra las claves criptográficas para la criptografía requerida empleada en el sistema de información de acuerdo con [asignación: requisitos definidos por la organización para la generación, distribución, almacenamiento, acceso y destrucción de claves].	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMK) necesarias no estén programadas para borrado en AWS Key Management Service (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenciales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenciales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMK) necesarias no estén programadas para borrado en AWS Key Management Service (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de informaci ón.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegi o mínimo y separació n de funciones con permisos y autorizac iones de acceso, ya que garantiza que los grupos de IAM tengan al menos un usuario de IAM. Una forma de incorporar el privilegi o mínimo es colocar a los usuarios de IAM en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de información.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de informaci ón.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomiend a que se utilicen políticas administr adas en lugar de políticas insertadas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de información.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de informaci ón.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	alb-http-to-https-comprobación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	elasticsearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service (OpenSearch Service).
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMK) necesarias no estén programadas para borrado en AWS Key Management Service (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenciales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenciales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	ec-2 ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	El sistema de información protege la confidencialidad Y la integridad de [asignación: información en reposo definida por la organización].	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	ec-2 volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicación de DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a internet para las cargas de trabajo dentro de las Amazon VPC puede reducir el acceso no deseado a su entorno.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterminado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB usa el servicio de escalado automático de aplicaciones de AWS para ajustar de manera automática a la capacidad de rendimiento aprovisionada en respuesta a los patrones de tráfico reales. Esto permite a una tabla o índice secundario global incrementar su capacidad de lectura y escritura aprovisionada para gestionar incrementos repentinos del tráfico sin limitaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	Regla de AWS Config	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignaci ón: tipos de ataques de denegación de servicio definidos por la organizac ión o referencias a las fuentes de dicha información] mediante la aplicació n de [asignación: medidas de seguridad definidas por la organización].	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELB) para poder conservar la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	vpc-vpn-2-tunnels-up	Para cumplir los requisitos de resiliencia, pueden implementarse túneles de Site-to-Site VPN redundantes. Se utilizan dos túneles para garantizar la conectividad en caso de que una de las conexiones de Site-to-Site VPN no esté disponible. Para protegerse frente a la pérdida de conectividad que se produciría si su puerta de enlace de cliente dejara de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN con la Amazon Virtual Private Cloud (Amazon VPC) y la puerta de enlace privada virtual con otro dispositivo de puerta de enlace de cliente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional dedicada para las operaciones de E/S de Amazon EBS. Esta optimización ofrece el mejor rendimiento para sus volúmenes de EBS, ya que reduce al mínimo la contención entre las operaciones de E/S de Amazon EBS y otro tráfico procedente de la instancia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando se habilitan las copias de seguridad automáticas, Amazon ElastiCache crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	ec-2 instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Amazon VPC para gestionar correctamente el acceso.
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicación de DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	elasticsearch-in-vpc-only	Gestione el acceso a la nube de AWS de manera que se garantice que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h Service dentro de una Amazon VPC garantiza una comunicación segura entre OpenSearc h Service y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de Internet, un dispositivo NAT o una conexión de VPN.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	Regla de AWS Config	Directrices
			deben asignarse a una VPC.
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidenc ialidad de los sistemas. Esta regla le permite configura r de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,338 9,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	alb-http-to-https-comprobación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicacio nes web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	s3- account-level-publ ic-access -bloques- periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterm inado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la nube de AWS de manera que garantice que no se asigne automáticamente una dirección IP pública a las subredes de Amazon Virtual Private Cloud (VPC). Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	s3- bucket-level-publi c-access -prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ec-2 instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Amazon VPC para gestionar correctamente el acceso.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicación de DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	elasticsearch-in-vpc-only	Gestione el acceso a la nube de AWS de manera que se garantice que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h Service dentro de una Amazon VPC garantiza una comunicación segura entre OpenSearc h Service y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de Internet, un dispositivo NAT o una conexión de VPN.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	Regla de AWS Config	Directrices
			deben asignarse a una VPC.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterm inado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la nube de AWS de manera que garantice que no se asigne automáticamente una dirección IP pública a las subredes de Amazon Virtual Private Cloud (VPC). Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmiti da.	alb-http-to-https-comprobación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmitida.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmitida.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmitida.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmitida.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8	El sistema de información protege la confidencialidad E integridad de la información transmiti da.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
SC-8(1)	El sistema de información implementa mecanismos criptográ ficos para [seleccio nar (una o más): impedir la divulgaci ón no autorizad a de información; detectar cambios en la información] durante la transmisi ón, a menos que esté protegida de otra manera con [asignación: proteccio nes físicas alternati vas definidas por la organización].	alb-http-to-https-comprobación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando se habilitan las copias de seguridad automáticas, Amazon ElastiCache crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de copia de seguridad de datos, asegúrese de que su plan de AWS Backup esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer los parámetros requiredFrequencyValue (valor predeterminado de Config: 1), requiredRetentionDays (valor predeterminado de Config: 35) y

ID de control	Descripción del control	Regla de AWS Config	Directrices
			requiredFrequencyUnit (valor predeterminado de Config: days). El valor real debe reflejar los requisitos de su organización.
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	fsx-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus sistemas de archivos de Amazon FSx formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	ec2-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	aurora-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	dynamodb-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	ebs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	efs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	rds-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un plan de AWSBackup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2(2)	La organización emplea mecanismos automatizados como mínimo mensualmente para determinar el estado de los componentes del sistema de información con respecto a la corrección de defectos.	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2(2)	La organización emplea mecanismos automatizados como mínimo mensualmente para determinar el estado de los componentes del sistema de información con respecto a la corrección de defectos.	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2(2)	La organización emplea mecanismos automatizados como mínimo mensualmente para determinar el estado de los componentes del sistema de información con respecto a la corrección de defectos.	ec2- -comprobar managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2(2)	La organización emplea mecanismos automatizados como mínimo mensualmente para determinar el estado de los componentes del sistema de información con respecto a la corrección de defectos.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(1)	La organización conecta y configura las herramientas individuales de detección de intrusos en un sistema de detección de intrusos que abarca todo el sistema de informaci ón.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	ec-2 instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente de forma continua para detectar actividades o condiciones inusuales o no autorizadas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente de forma continua para detectar actividades o condiciones inusuales o no autorizadas.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente de forma continua para detectar actividades o condiciones inusuales o no autorizadas.	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente de forma continua para detectar actividades o condiciones inusuales o no autorizadas.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	guardduty-non-archived-findings	Amazon GuardDuty le ayuda a comprender el efecto de un incidente al clasificar los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional daysLowSev (valor predeterminado de Config: 30), daysMediumSev (valor predeterminado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicaciones web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	ec-2 instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	api-gw-associated-with-guerra	AWS WAF permite configurar un conjunto de reglas (denominadas lista de control de acceso web (ACL web) que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-7	La organización emplea herramientas de verificación de la integridad para detectar cambios no autorizados en [asignación: software, firmware e información definidos por la organización].	cloud-trail-log-file-habilitada para validación	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-7(1)	El sistema de información comprueba la integridad de los eventos relevante s para la seguridad al menos una vez al mes.	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administr ación de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-7(1)	El sistema de información comprueba la integridad de los eventos relevantes para la seguridad al menos una vez al mes.	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-7(1)	El sistema de información comprueba la integridad de los eventos relevantes para la seguridad al menos una vez al mes.	cloud-trail-log-file-habilitada para validación	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-5(1)	La organización emplea herramientas de análisis de vulnerabilidades que incluyen la capacidad de actualizar fácilmente las vulnerabilidades del sistema de información que se van a analizar. Directriz complementaria: las vulnerabilidades que se van a analizar deben actualizarse rápidamente a medida que se descubran, anuncien y desarrollen nuevos métodos de análisis. Este proceso de actualización ayuda a garantizar que las posibles vulnerabilidades del sistema de información se identifiquen y aborden lo antes posible. Controles relacionados: SI-3 y SI-7.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-5(1)	La organización emplea herramientas de análisis de vulnerabilidades que incluyen la capacidad de actualizar fácilmente las vulnerabilidades del sistema de información que se van a analizar. Directriz complementaria: las vulnerabilidades que se van a analizar deben actualizarse rápidamente a medida que se descubran, anuncien y desarrollen nuevos métodos de análisis. Este proceso de actualización ayuda a garantizar que las posibles vulnerabilidades del sistema de información se identifiquen y aborden lo antes posible. Controles relacionados: SI-3 y SI-7.	guardduty-non-archived-findings	Amazon GuardDuty le ayuda a comprender el efecto de un incidente al clasificar los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional daysLowSev (valor predeterminado de Config: 30), daysMediumSev (valor predeterminado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-5(1)	La organización emplea herramientas de análisis de vulnerabilidades que incluyen la capacidad de actualizar fácilmente las vulnerabilidades del sistema de información que se van a analizar. Directriz complementaria: las vulnerabilidades que se van a analizar deben actualizarse rápidamente a medida que se descubran, anuncien y desarrollen nuevos métodos de análisis. Este proceso de actualización ayuda a garantizar que las posibles vulnerabilidades del sistema de información se identifiquen y aborden lo antes posible. Controles relacionados: SI-3 y SI-7.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una misión o necesidad empresari al de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [asignación: frecuencia definida por la organizac ión] y elimina las excepciones que ya no cuentan con el apoyo de una misión explícita o necesidad	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	empresarial. Directriz complementaria: control relacionado: SC-8.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administrada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una misión o necesidad empresarial de apoyo y la duración de esa necesidad; y (e) Revisa las excepciones a la política de flujo de tráfico [asignación: frecuencia definida por la organización] y elimina las excepciones que ya no cuentan con el apoyo de una misión explícita o necesidad	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	empresarial. Directriz complementaria: control relacionado: SC-8.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una misión o necesidad empresari al de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [asignación: frecuencia definida por la organizac ión] y elimina las excepciones que ya no cuentan con el apoyo de una misión explícita o necesidad	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	empresarial. Directriz complementaria: control relacionado: SC-8.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una misión o necesidad empresari al de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [asignación: frecuencia definida por la organizac ión] y elimina las excepciones que ya no cuentan con el apoyo de una misión explícita o necesidad	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	empresarial. Directriz complementaria: control relacionado: SC-8.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una misión o necesidad empresari al de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [asignación: frecuencia definida por la organizac ión] y elimina las excepciones que ya no cuentan con el apoyo de una misión explícita o necesidad	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	empresarial. Directriz complementaria: control relacionado: SC-8.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7(4)	La organización: (a) Implementa una interfaz administrada para cada servicio de telecomunicaciones externo; (b) Establece una política de flujo de tráfico para cada interfaz administr ada; (c) Protege la confidencialidad e integridad de la información que se transmite a través de cada interfaz; (d) Documenta cada excepción a la política de flujo de tráfico con una misión o necesidad empresari al de apoyo y la duración de esa necesidad; y (e) Revisa las excepcion es a la política de flujo de tráfico [asignación: frecuencia definida por la organizac ión] y elimina las excepciones que ya no cuentan con el apoyo de una misión explícita o necesidad	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	empresarial. Directriz complementaria: control relacionado: SC-8.		
SC-7(5)	El sistema de información de las interfaces administradas deniega el tráfico de comunicaciones de red de forma predeterminada y permite el tráfico de comunicaciones de red por excepción (es decir, deniega todo, permite por excepción). Directriz complementaria: esta mejora del control se aplica al tráfico de comunicaciones de red tanto entrante como saliente. Una política de tráfico de comunicaciones de red que lo deniega todo y permite por excepción garantiza que solo se permitan las conexiones esenciales y autorizadas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(7)	La organización (a) establece y administr a las cuentas de usuario con privilegi os, de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de información y los privilegios en roles; (b) supervisa la asignación de roles con privilegios; y (c) toma [asignación: medidas definidas por la organización] cuando las asignacio nes de roles con privilegios ya no son adecuadas. Directriz complemen taria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separació n de funciones con permisos y autorizac iones de acceso, lo que impide que las políticas incluyan acciones bloqueada s en todas las claves del AWS Key Management Service. Tener más privilegi os de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones . Esta regla le permite establecer el parámetro blockedAc tionsPatterns. (Valor de las prácticas recomendadas de seguridad básica de AWS: kms:Decrypt, kms:ReEncryptFrom) . Los valores reales deben reflejar las

ID de control	Descripción del control	Regla de AWS Config	Directrices
	os a realizar. Estos roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(7)	La organización (a) establece y administra las cuentas de usuario con privilegios, de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de información y los privilegios en roles; (b) supervisa la asignación de roles con privilegios; y (c) toma [asignación: medidas definidas por la organización] cuando las asignaciones de roles con privilegios ya no son adecuadas. Directriz complementaria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	os a realizar. Estos roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(7)	La organización (a) establece y administra las cuentas de usuario con privilegios, de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de información y los privilegios en roles; (b) supervisa la asignación de roles con privilegios; y (c) toma [asignación: medidas definidas por la organización] cuando las asignaciones de roles con privilegios ya no son adecuadas. Directriz complementaria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	os a realizar. Estos roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(7)	La organización (a) establece y administr a las cuentas de usuario con privilegi os, de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de información y los privilegios en roles; (b) supervisa la asignación de roles con privilegios; y (c) toma [asignación: medidas definidas por la organización] cuando las asignacio nes de roles con privilegios ya no son adecuadas. Directriz complemen taria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegi o mínimo y separació n de funciones con permisos y autorizac iones de acceso, ya que garantiza que los grupos de IAM tengan al menos un usuario de IAM. Una forma de incorporar el privilegi o mínimo es colocar a los usuarios de IAM en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	os a realizar. Estos roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(7)	La organización (a) establece y administr a las cuentas de usuario con privilegi os, de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de información y los privilegios en roles; (b) supervisa la asignación de roles con privilegios; y (c) toma [asignación: medidas definidas por la organización] cuando las asignacio nes de roles con privilegios ya no son adecuadas. Directriz complemen taria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada que permita acciones bloqueada s en todas las claves de AWS Key Management Service. AWS recomienda que utilice políticas administradas en lugar de políticas insertadas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el parámetro blockedActionsPatt erns. (Valor de las prácticas recomenda das de seguridad básica de AWS: kms:Decrypt,

ID de control	Descripción del control	Regla de AWS Config	Directrices
	os a realizar. Estos roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(7)	La organización (a) establece y administr a las cuentas de usuario con privilegi os, de acuerdo con un esquema de acceso basado en roles que organiza el acceso permitido al sistema de información y los privilegios en roles; (b) supervisa la asignación de roles con privilegios; y (c) toma [asignación: medidas definidas por la organización] cuando las asignacio nes de roles con privilegios ya no son adecuadas. Directriz complemen taria: los roles con privilegios son roles definidos por la organización que se asignan a personas y que les permiten realizar ciertos roles relevantes para la seguridad que los usuarios comunes no están autorizad	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomiend a que se utilicen políticas administr adas en lugar de políticas insertadas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	os a realizar. Estos roles con privilegios incluyen, por ejemplo, la administración de claves, la administr ación de cuentas, la administración de redes y sistemas, la administración de bases de datos y la administración web.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcio nan la información necesaria para las acciones correctivas sin revelar informaci ón que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignaci ón: al personal o los roles definidos por la organización]. Directriz complemen taria: las organizac iones considera n detenidamente la estructura y el contenido de los mensajes de error. La medida en que los sistemas de informaci ón son capaces de identificar y gestionar las condiciones de error depende de la política de la organización y los requisitos operativo	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	s. Entre los datos que podrían aprovecha r los adversarios figuran, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como el nombre de usuario, la informaci ón sobre la misión o la empresa que puede derivarse de la información registrad a (si no se indica explícitamente) y la información personal, como números de cuenta, números de la Seguridad Social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcio nan la información necesaria para las acciones correctivas sin revelar informaci ón que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignaci ón: al personal o los roles definidos por la organización]. Directriz complemen taria: las organizac iones considera n detenidamente la estructura y el contenido de los mensajes de error. La medida en que los sistemas de informaci ón son capaces de identificar y gestionar las condiciones de error depende de la política de la organización y los requisitos operativo	codebuild-project-logging-enabled	Asegúrese de que el registro de proyectos de AWS CodeBuild esté habilitado para que los registros de salida de compilaci ón se envíen a Amazon CloudWatc h o Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	s. Entre los datos que podrían aprovecha r los adversarios figuran, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como el nombre de usuario, la informaci ón sobre la misión o la empresa que puede derivarse de la información registrad a (si no se indica explícitamente) y la información personal, como números de cuenta, números de la Seguridad Social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcio nan la información necesaria para las acciones correctivas sin revelar informaci ón que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignaci ón: al personal o los roles definidos por la organización]. Directriz complemen taria: las organizac iones considera n detenidamente la estructura y el contenido de los mensajes de error. La medida en que los sistemas de informaci ón son capaces de identificar y gestionar las condiciones de error depende de la política de la organización y los requisitos operativo	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	s. Entre los datos que podrían aprovecha r los adversarios figuran, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como el nombre de usuario, la informaci ón sobre la misión o la empresa que puede derivarse de la información registrad a (si no se indica explícitamente) y la información personal, como números de cuenta, números de la Seguridad Social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcionan la información necesaria para las acciones correctivas sin revelar información que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignación: al personal o los roles definidos por la organización]. Directriz complementaria: las organizaciones considerarán detenidamente la estructura y el contenido de los mensajes de error. La medida en que los sistemas de información son capaces de identificar y gestionar las condiciones de error depende de la política de la organización y los requisitos operativo	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	s. Entre los datos que podrían aprovecha r los adversarios figuran, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como el nombre de usuario, la informaci ón sobre la misión o la empresa que puede derivarse de la información registrad a (si no se indica explícitamente) y la información personal, como números de cuenta, números de la Seguridad Social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcionan la información necesaria para las acciones correctivas sin revelar información que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignación: al personal o los roles definidos por la organización]. Directriz complementaria: las organizaciones considerarán detenidamente la estructura y el contenido de los mensajes de error. La medida en que los sistemas de información son capaces de identificar y gestionar las condiciones de error depende de la política de la organización y los requisitos operativo	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	s. Entre los datos que podrían aprovecha r los adversarios figuran, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como el nombre de usuario, la informaci ón sobre la misión o la empresa que puede derivarse de la información registrad a (si no se indica explícitamente) y la información personal, como números de cuenta, números de la Seguridad Social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-11	El sistema de información: a. Genera mensajes de error que proporcionan la información necesaria para las acciones correctivas sin revelar información que pueda ser aprovechada por los adversarios; y b. Revela los mensajes de error únicamente [asignación: al personal o los roles definidos por la organización]. Directriz complementaria: las organizaciones considerarán detenidamente la estructura y el contenido de los mensajes de error. La medida en que los sistemas de información son capaces de identificar y gestionar las condiciones de error depende de la política de la organización y los requisitos operativo	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y que se transmitan a los registros de Amazon CloudWatch para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	s. Entre los datos que podrían aprovecha r los adversarios figuran, por ejemplo, los intentos de inicio de sesión erróneos con contraseñas introducidas por error como el nombre de usuario, la informaci ón sobre la misión o la empresa que puede derivarse de la información registrad a (si no se indica explícitamente) y la información personal, como números de cuenta, números de la Seguridad Social y números de tarjetas de crédito. Además, los mensajes de error pueden proporcionar un canal encubiert o para transmiti r información. Controles relaciona dos: AU-2, AU-3 y SC-31. Mejoras del control: ninguna. Referencias: ninguna.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-3	La organización: a. Emplea mecanismos de protección de códigos maliciosos en los puntos de entrada y salida del sistema de información para detectar y erradicar los códigos malicioso s; b. Actualiza los mecanismos de protección contra los códigos malicioso s cada vez que hay nuevas versiones disponibles, de conformidad con la política y los procedimientos de gestión de la configuración de la organización; c. Configura los mecanismos de protección contra códigos malicioso s para: 1. Realizar análisis periódicos del sistema de informaci ón [asignación: frecuencia definida por la organización] y análisis en tiempo	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales de autenticación AWS_ACCES S_KEY_ID y AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyecto de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	real de los archivos de fuentes externas en [seleccionar (uno o más); punto de conexión; puntos de entrada y salida de la red] a medida que los archivos se descargan, abren o ejecutan de acuerdo con la política de seguridad de la organizac ión; y 2. [Seleccio nar (una o más): bloquear el código malicioso; poner en cuarentena el código malicioso; enviar una alerta al administr ador; [asignación: acción definida por la organizac ión]] en respuesta a la detección de código malicioso; y d. Aborda la aparición de falsos positivos durante la detección y erradicación de códigos maliciosos y su posible impacto en la disponibilidad del sistema de		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	información. Directriz complementaria: los puntos de entrada y salida del sistema de información incluyen, por ejemplo, firewalls , servidores de correo electrónico, servidore s web, servidores proxy, servidores de acceso remoto, estaciones de trabajo, equipos portátile s y dispositivos móviles. Los códigos maliciosos incluyen, por ejemplo, virus, gusanos, troyanos y spyware. El código malicioso también puede codificarse en varios formatos (por ejemplo, UUENCODE o Unicode), incluirse en archivos comprimidos u ocultos y ocultarse en archivos mediante esteganografía. El código malicioso se puede transport ar por diferentes medios, como, por ejemplo, accesos		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	a la web, correo electrónico, archivos adjuntos de correo electrónico y dispositivos de almacenamiento portátiles. Las inserciones de código malicioso se producen mediante la explotación de las vulnerabilidades del sistema de información. Los mecanismos de protección contra códigos maliciosos incluyen, por ejemplo, las definiciones de firmas antivirus y las tecnologías basadas en la reputación. Existen diversas tecnologías y métodos para limitar o eliminar los efectos de los códigos maliciosos. La gestión generalizada de la configuración y los controles exhaustivos de integridad del software pueden ser eficaces para impedir la ejecución de código no autorizado.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	Además del software comercial disponible en el mercado, también puede haber códigos maliciosos en el software personalizado. Esto podría incluir, por ejemplo, bombas lógicas, puertas traseras y otros tipos de ciberataques que pueden afectar a las misiones o las funciones empresariales de la organización. Los mecanismos tradicionales de protección contra códigos maliciosos no siempre detectan dicho código. En estas situaciones, las organizaciones se basan más bien en otras medidas de seguridad, como las prácticas de codificación seguras, la gestión y el control de la configuración, los procesos de compra de confianza y las prácticas		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de monitoreo, para garantizar que el software no desempeñe funciones distintas de las previstas. Las organizaciones pueden determinar que, en respuesta a la detección de código malicioso, se puedan garantizar diferente s acciones. Por ejemplo, las organizac iones pueden definir acciones en respuesta a la detección de códigos maliciosos durante los análisis periódicos, acciones en respuesta a la detección de descargas maliciosa s o acciones en respuesta a la detección de código malicioso al intentar abrir o ejecutar archivos. Controles relacionados: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2,		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	SI-4 y SI-7. Referencias: Publicación especial 800-83 del NIST.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-3	La organización: a. Emplea mecanismos de protección de códigos maliciosos en los puntos de entrada y salida del sistema de información para detectar y erradicar los códigos malicioso s; b. Actualiza los mecanismos de protección contra los códigos malicioso s cada vez que hay nuevas versiones disponibles, de conformidad con la política y los procedimientos de gestión de la configuración de la organización; c. Configura los mecanismos de protección contra códigos malicioso s para: 1. Realizar análisis periódicos del sistema de informaci ón [asignación: frecuencia definida por la organización] y análisis en tiempo	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio de origen de GitHub o Bitbucket no contenga tokens de acceso personal, nombres de usuario ni contraseñ as en los entornos de proyectos de AWS Codebuild. En lugar de tokens de acceso personal o un nombre de usuario y contraseñ a, utilice OAuth a fin de conceder autorizac ión para el acceso a repositorios de GitHub o Bitbucket.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	real de los archivos de fuentes externas en [seleccionar (uno o más); punto de conexión; puntos de entrada y salida de la red] a medida que los archivos se descargan, abren o ejecutan de acuerdo con la política de seguridad de la organizac ión; y 2. [Seleccio nar (una o más): bloquear el código malicioso; poner en cuarentena el código malicioso; enviar una alerta al administr ador; [asignación: acción definida por la organizac ión]] en respuesta a la detección de código malicioso; y d. Aborda la aparición de falsos positivos durante la detección y erradicación de códigos maliciosos y su posible impacto en la disponibilidad del sistema de		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	información. Directriz complementaria: los puntos de entrada y salida del sistema de información incluyen, por ejemplo, firewalls , servidores de correo electrónico, servidore s web, servidores proxy, servidores de acceso remoto, estaciones de trabajo, equipos portátile s y dispositivos móviles. Los códigos maliciosos incluyen, por ejemplo, virus, gusanos, troyanos y spyware. El código malicioso también puede codificarse en varios formatos (por ejemplo, UUENCODE o Unicode), incluirse en archivos comprimidos u ocultos y ocultarse en archivos mediante esteganografía. El código malicioso se puede transport ar por diferentes medios, como, por ejemplo, accesos		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	a la web, correo electrónico, archivos adjuntos de correo electrónico y dispositivos de almacenamiento portátiles. Las inserciones de código malicioso se producen mediante la explotación de las vulnerabilidades del sistema de información. Los mecanismos de protección contra códigos maliciosos incluyen, por ejemplo, las definiciones de firmas antivirus y las tecnologías basadas en la reputación. Existen diversas tecnologías y métodos para limitar o eliminar los efectos de los códigos maliciosos. La gestión generalizada de la configuración y los controles exhaustivos de integridad del software pueden ser eficaces para impedir la ejecución de código no autorizado.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	Además del software comercial disponible en el mercado, también puede haber códigos maliciosos en el software personalizado. Esto podría incluir, por ejemplo, bombas lógicas, puertas traseras y otros tipos de ciberataques que pueden afectar a las misiones o las funciones empresariales de la organización. Los mecanismos tradicionales de protección contra códigos maliciosos no siempre detectan dicho código. En estas situaciones, las organizaciones se basan más bien en otras medidas de seguridad, como las prácticas de codificación seguras, la gestión y el control de la configuración, los procesos de compra de confianza y las prácticas		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de monitoreo, para garantizar que el software no desempeñe funciones distintas de las previstas. Las organizaciones pueden determinar que, en respuesta a la detección de código malicioso, se puedan garantizar diferente s acciones. Por ejemplo, las organizac iones pueden definir acciones en respuesta a la detección de códigos maliciosos durante los análisis periódicos, acciones en respuesta a la detección de descargas maliciosa s o acciones en respuesta a la detección de código malicioso al intentar abrir o ejecutar archivos. Controles relacionados: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2,		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	SI-4 y SI-7. Referencias: Publicación especial 800-83 del NIST.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-5	La organización: a. Recibe alertas, avisos y políticas de seguridad del sistema de información de [asignación: organizaciones externas definidas por la organización] de forma continua; b. Genera alertas, avisos y políticas de seguridad internas según se considere necesario; c. Difunde alertas, avisos y políticas de seguridad entre: [seleccionar (una o más): [asignación: el personal o los roles definidos por la organización]; [asignación: los elementos definidos por la organización dentro de la organización]; [asignación: las organizaciones externas definidas por la organización]]; y d. Implementa las políticas de seguridad de acuerdo con los	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	plazos establecidos o notifica a la organizac ión emisora el grado de incumplimiento. Directriz complemen taria: el equipo de respuesta ante emergencias informáti cas de los Estados Unidos (US-CERT, por sus siglas en inglés) genera alertas y avisos de seguridad para mantener al gobierno federal al corriente de la situación. La Oficina de Administración y Presupuestos de Estados Unidos (OMB, por sus siglas en inglés) u otras organizaciones con la autoridad y responsab ilidad correspon dientes publican las políticas de seguridad . El cumplimiento de las directivas de seguridad es esencial debido a la naturalez a crítica de muchas de estas políticas y a los posibles efectos		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	adversos inmediatos en las operaciones y los activos de la organización, las personas, otras organizaciones y el país si las políticas no se implementan de manera oportuna. Las organizaciones externas son, por ejemplo, socios comerciales o de misión externos, socios de la cadena de suministro, proveedores de servicios externos y otras organizaciones homólogas o de apoyo. Control relacionado: SI-2. Referencias: Publicación especial 800-40 del NIST.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-5	La organización: a. Recibe alertas, avisos y políticas de seguridad del sistema de información de [asignación: organizaciones externas definidas por la organización] de forma continua; b. Genera alertas, avisos y políticas de seguridad internas según se considere necesario; c. Difunde alertas, avisos y políticas de seguridad entre: [seleccionar (una o más): [asignación: el personal o los roles definidos por la organización]; [asignación: los elementos definidos por la organización dentro de la organización]; [asignación: las organizaciones externas definidas por la organización]]; y d. Implementa las políticas de seguridad de acuerdo con los	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	plazos establecidos o notifica a la organizac ión emisora el grado de incumplimiento. Directriz complemen taria: el equipo de respuesta ante emergencias informáti cas de los Estados Unidos (US-CERT, por sus siglas en inglés) genera alertas y avisos de seguridad para mantener al gobierno federal al corriente de la situación. La Oficina de Administración y Presupuestos de Estados Unidos (OMB, por sus siglas en inglés) u otras organizaciones con la autoridad y responsab ilidad correspon dientes publican las políticas de seguridad . El cumplimiento de las directivas de seguridad es esencial debido a la naturalez a crítica de muchas de estas políticas y a los posibles efectos		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	adversos inmediatos en las operaciones y los activos de la organización, las personas, otras organizaciones y el país si las políticas no se implementan de manera oportuna. Las organizaciones externas son, por ejemplo, socios comerciales o de misión externos, socios de la cadena de suministro, proveedores de servicios externos y otras organizaciones homólogas o de apoyo. Control relacionado: SI-2. Referencias: Publicación especial 800-40 del NIST.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-5	La organización: a. Recibe alertas, avisos y políticas de seguridad del sistema de informaci ón de [asignaci ón: organizaciones externas definidas por la organización] de forma continua; b. Genera alertas, avisos y políticas de seguridad internas según se considere necesario; c. Difunde alertas, avisos y políticas de seguridad entre: [seleccionar (una o más): [asignaci ón: el personal o los roles definidos por la organizac ión]; [asignación: los elementos definidos por la organización dentro de la organizac ión]; [asignación: las organizaciones externas definidas por la organización]]; y d. Implementa las políticas de seguridad de acuerdo con los	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	plazos establecidos o notifica a la organizac ión emisora el grado de incumplimiento. Directriz complemen taria: el equipo de respuesta ante emergencias informáti cas de los Estados Unidos (US-CERT, por sus siglas en inglés) genera alertas y avisos de seguridad para mantener al gobierno federal al corriente de la situación. La Oficina de Administración y Presupuestos de Estados Unidos (OMB, por sus siglas en inglés) u otras organizaciones con la autoridad y responsab ilidad correspon dientes publican las políticas de seguridad . El cumplimiento de las directivas de seguridad es esencial debido a la naturalez a crítica de muchas de estas políticas y a los posibles efectos		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	adversos inmediatos en las operaciones y los activos de la organización, las personas, otras organizaciones y el país si las políticas no se implementan de manera oportuna. Las organizaciones externas son, por ejemplo, socios comerciales o de misión externos, socios de la cadena de suministro, proveedores de servicios externos y otras organizaciones homólogas o de apoyo. Control relacionado: SI-2. Referencias: Publicación especial 800-40 del NIST.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-5	La organización: a. Recibe alertas, avisos y políticas de seguridad del sistema de información de [asignación: organizaciones externas definidas por la organización] de forma continua; b. Genera alertas, avisos y políticas de seguridad internas según se considere necesario; c. Difunde alertas, avisos y políticas de seguridad entre: [seleccionar (una o más): [asignación: el personal o los roles definidos por la organización]; [asignación: los elementos definidos por la organización dentro de la organización]; [asignación: las organizaciones externas definidas por la organización]]; y d. Implementa las políticas de seguridad de acuerdo con los	guardduty-non-archived-findings	Amazon GuardDuty le ayuda a comprender el efecto de un incidente al clasificar los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional daysLowSev (valor predeterminado de Config: 30), daysMediumSev (valor predeterminado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	plazos establecidos o notifica a la organizac ión emisora el grado de incumplimiento. Directriz complemen taria: el equipo de respuesta ante emergencias informáti cas de los Estados Unidos (US-CERT, por sus siglas en inglés) genera alertas y avisos de seguridad para mantener al gobierno federal al corriente de la situación. La Oficina de Administración y Presupuestos de Estados Unidos (OMB, por sus siglas en inglés) u otras organizaciones con la autoridad y responsab ilidad correspon dientes publican las políticas de seguridad . El cumplimiento de las directivas de seguridad es esencial debido a la naturalez a crítica de muchas de estas políticas y a los posibles efectos		

ID de control	Descripción del control	Regla de AWS Config	Directrices
	adversos inmediatos en las operaciones y los activos de la organización, las personas, otras organizaciones y el país si las políticas no se implementan de manera oportuna. Las organizaciones externas son, por ejemplo, socios comerciales o de misión externos, socios de la cadena de suministro, proveedores de servicios externos y otras organizaciones homólogas o de apoyo. Control relacionado: SI-2. Referencias: Publicación especial 800-40 del NIST.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	codebuild-project-logging-enabled	Asegúrese de que el registro de proyectos de AWS CodeBuild esté habilitado para que los registros de salida de compilaci ón se envíen a Amazon CloudWatc h o Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	codebuild-project-logging-enabled	Asegúrese de que el registro de proyectos de AWS CodeBuild esté habilitado para que los registros de salida de compilaci ón se envíen a Amazon CloudWatc h o Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en todos los componentes del sistema de informaci ón y de red en los que se despliega o está disponibl e la capacidad de auditoría c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	codebuild-project-logging-enabled	Asegúrese de que el registro de proyectos de AWS CodeBuild esté habilitado para que los registros de salida de compilaci ón se envíen a Amazon CloudWatc h o Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: eventos de inicio de sesión de cuenta correcto o incorrecto, eventos de administración de cuentas, acceso a objetos, cambio de política, funciones con privilegios, seguimien to de procesos y eventos del sistema. Para las aplicacio nes web: toda la actividad del administr ador, las comprobac iones de autentica ción, las comprobac iones de autorización, las eliminaciones de datos, el acceso a los datos, los cambios de datos y los cambios de permisos. d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [el	codebuild-project-logging-enabled	Asegúrese de que el registro de proyectos de AWS CodeBuild esté habilitado para que los registros de salida de compilaci ón se envíen a Amazon CloudWatc h o Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	subconjunto definido por la organización de los eventos auditable s definidos en el AU-2 a. deberá auditarse continuamente para cada evento identific ado].		
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	codebuild-project-logging-enabled	Asegúrese de que el registro de proyectos de AWS CodeBuild esté habilitado para que los registros de salida de compilaci ón se envíen a Amazon CloudWatc h o Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	codebuild-project-logging-enabled	Asegúrese de que el registro de proyectos de AWS CodeBuild esté habilitado para que los registros de salida de compilaci ón se envíen a Amazon CloudWatc h o Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

Plantilla

La plantilla está disponible en GitHub: Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 1).

Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 2)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear comprobaciones de control de seguridad, operativas o de optimización de costos mediante reglas de AWS Config administradas o personalizadas y acciones correctivas de AWS Config. Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación se proporciona un ejemplo de asignación entre el Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP, por sus siglas en inglés) y las reglas de AWS Config administradas. Cada regla de Config se aplica a un recurso de AWS específico que está relacionado con uno o más controles del FedRAMP. Un control del FedRAMP puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-02 (11)	El sistema de información aplica las circunstancias o las condiciones de uso definidas por la organización en las cuentas del sistema definidas por la organización.	guardduty-enabled-centralized	Utilice Amazon GuardDuty para supervisar el uso de las credencia les a corto plazo asociadas a los roles de instancias de IAM. Amazon GuardDuty puede comprobar la exfiltración de credenciales en los perfiles de instancia de IAM mediante la comprobación UnauthorizedAccess.
AC-02 (12)(a)	La organización: a. Monitorea las cuentas del sistema de información para detectar [asignaci ón: un uso atípico definido por la organización].	cloudtrail-security-trail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a

ID de control	Descripción del control	Regla de AWS Config	Directrices
			un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.
AC-06 (03)	La organización autoriza el acceso a la red al personal asignado solo cuando eso sea necesario para completar la tarea de acceso del plan de seguridad.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-06 (03)	La organización autoriza el acceso a la red a [asignación: comandos con privilegios definidos por la organización] solo para [asignación: necesidades operativas apremiantes definidas por la organización] y documenta los motivos de dicho acceso en el plan de seguridad del sistema.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-06 (03)	La organización autoriza el acceso a la red a [asignación: comandos con privilegios definidos por la organización] solo para [asignación: necesidades operativas apremiantes definidas por la organización] y documenta los motivos de dicho acceso en el plan de seguridad del sistema.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la nube de AWS de manera que garantice que no se asigne automáticamente una dirección IP pública a las subredes de Amazon Virtual Private Cloud (VPC). Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-06 (03)	La organización autoriza el acceso a la red a [asignación: comandos con privilegios definidos por la organización] solo para [asignación: necesidades operativas apremiantes definidas por la organización] y documenta los motivos de dicho acceso en el plan de seguridad del sistema.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
AC-06 (03)	La organización autoriza el acceso a la red a [asignación: comandos con privilegios definidos por la organización] solo para [asignación: necesidades operativas apremiantes definidas por la organización] y documenta los motivos de dicho acceso en el plan de seguridad del sistema.	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-06 (03)	La organización autoriza el acceso a la red a [asignación: comandos con privilegios definidos por la organización] solo para [asignación: necesidades operativas apremiantes definidas por la organización] y documenta los motivos de dicho acceso en el plan de seguridad del sistema.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-06 (03)	La organización autoriza el acceso a la red a [asignación: comandos con privilegios definidos por la organización] solo para [asignación: necesidades operativas apremiantes definidas por la organización] y documenta los motivos de dicho acceso en el plan de seguridad del sistema.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-06 (03)	La organización autoriza el acceso a la red a [asignación: comandos con privilegios definidos por la organización] solo para [asignación: necesidades operativas apremiantes definidas por la organización] y documenta los motivos de dicho acceso en el plan de seguridad del sistema.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.
AC-06 (03)	La organización autoriza el acceso a la red a [asignación: comandos con privilegios definidos por la organización] solo para [asignación: necesidades operativas apremiantes definidas por la organización] y documenta los motivos de dicho acceso en el plan de seguridad del sistema.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-06 (03)	La organización autoriza el acceso a la red a [asignación: comandos con privilegios definidos por la organización] solo para [asignación: necesidades operativas apremiantes definidas por la organización] y documenta los motivos de dicho acceso en el plan de seguridad del sistema.	eks-endpoint-no-public-acceso	Administre el acceso al clúster de Amazon Elastic Kubernetes Service (Amazon EKS) asegurándose de que el punto de conexión del servidor de API de Kubernetes no sea de acceso público. Si limita el acceso público al punto de conexión del servidor de API de Kubernetes, puede reducir el riesgo de acceso no autorizado al clúster de EKS y sus recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-05 (02)	Cuando el volumen de almacenamiento de registros de auditoría asignado alcanza el porcentaj e establecido de la capacidad máxima de almacenam iento de registros de auditoría en el repositorio, el sistema de información envía una advertencia al personal correspon diente dentro del tiempo establecido.	cloudwatch-alarm-a ction-check	Las alarmas de Amazon CloudWatc h avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluació n. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActi onRequired (valor predeterminado de Config: True), insuffici entDataActionRequi red (valor predeterm inado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y que se transmitan a los registros de Amazon CloudWatch para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (04)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (05)	La organización integra el análisis de los registros de auditoría con el análisis de la información de escaneo de vulnerabilidades, los datos de rendimiento y los datos de supervisión del sistema para mejorar aún más la capacidad de identificación de actividades inapropiadas o inusuales.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (05)	La organización integra el análisis de los registros de auditoría con el análisis de [selección (una o más): la información de escaneo de vulnerabilidades; los datos de rendimiento; los datos de supervisión del sistema; [asignación: los datos o la información definidos por la organización y recopilados de otros orígenes]] para mejorar aún más la capacidad de identificación de actividades inapropiadas o inusuales.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (07)	La organización especifica las acciones permitida s para cada proceso del sistema, rol y usuario asociado a la revisión, el análisis y la presentación de informes sobre los datos de los registros de auditoría.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomiend a que se utilicen políticas administr adas en lugar de políticas insertadas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-06 (07)	La organización especifica las acciones permitidas para cada [selección (una o más): proceso del sistema; rol; usuario] asociado a la revisión, el análisis y la presentación de informes sobre los datos de los registros de auditoría.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-09 (02)	El sistema de información implementa mecanismos criptográficos para proteger la integridad de la información y las herramientas de auditoría.	cloud-trail-log-file-habilitada para validación	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-09 (02)	El sistema de información implementa mecanismos criptográficos para proteger la integridad de la información y las herramientas de auditoría.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
AU-09 (02)	El sistema de información implementa mecanismos criptográficos para proteger la integridad de la información y las herramientas de auditoría.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.
AU-09 (02)	El sistema de información implementa mecanismos criptográficos para proteger la integridad de la información y las herramientas de auditoría.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-09 (03)	El sistema de información proporciona evidencia irrefutable de que una persona ha llevado a cabo.	cloud-trail-log-file-habilitada para validación	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-09 (03)	El sistema de información limita el acceso a la red a los datos del registro de auditoría.	rastro de nubes -S3-bucket-public-access-prohibited	Se asegura de que los buckets de S3 empleados para almacenar registros de CloudTrail no sean de acceso público.
AU-10	El sistema de información proporcio na evidencia irrefutab le de que una persona (o un proceso en nombre de una persona) ha llevado a cabo [asignación: medidas definidas por la organización cuya autoría no es posible rechazar].	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-10	El sistema de información proporcio na evidencia irrefutab le de que una persona (o un proceso en nombre de una persona) ha llevado a cabo [asignación: medidas definidas por la organización cuya autoría no es posible rechazar].	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-10	El sistema de información proporcio na evidencia irrefutab le de que una persona (o un proceso en nombre de una persona) ha llevado a cabo [asignación: medidas definidas por la organización cuya autoría no es posible rechazar].	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AU-12	La organización recopila los registros de auditoría de [asignación: componentes del sistema definidos por la organización] en un registro de auditoría (lógico o físico) de todo el sistema que se sincroniza con el [asignación: nivel de tolerancia definido por la organización para la relación entre las marcas de tiempo de los registros individuales de la pista de auditoría].	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	La organización recopila los registros de auditoría de [asignación: componentes del sistema definidos por la organización] en un registro de auditoría (lógico o físico) de todo el sistema que se sincroniza con el [asignación: nivel de tolerancia definido por la organización para la relación entre las marcas de tiempo de los registros individuales de la pista de auditoría].	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	La organización recopila los registros de auditoría de [asignación: componentes del sistema definidos por la organización] en un registro de auditoría (lógico o físico) de todo el sistema que se sincroniza con el [asignación: nivel de tolerancia definido por la organización para la relación entre las marcas de tiempo de los registros individuales de la pista de auditoría].	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	La organización recopila los registros de auditoría de [asignación: componentes del sistema definidos por la organización] en un registro de auditoría (lógico o físico) de todo el sistema que se sincroniza con el [asignación: nivel de tolerancia definido por la organización para la relación entre las marcas de tiempo de los registros individuales de la pista de auditoría].	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	La organizac ión recopila los registros de auditoría de [asignación: componentes del sistema definidos por la organización] en un registro de auditoría (lógico o físico) de todo el sistema que se sincroniza con el [asignación: nivel de tolerancia definido por la organización para la relación entre las marcas de tiempo de los registros individua les de la pista de auditoría].	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
AU-12	La organizac ión recopila los registros de auditoría de [asignación: componentes del sistema definidos por la organización] en un registro de auditoría (lógico o físico) de todo el sistema que se sincroniza con el [asignación: nivel de tolerancia definido por la organización para la relación entre las marcas de tiempo de los registros individua les de la pista de auditoría].	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	La organizac ión recopila los registros de auditoría de [asignación: componentes del sistema definidos por la organización] en un registro de auditoría (lógico o físico) de todo el sistema que se sincroniza con el [asignación: nivel de tolerancia definido por la organización para la relación entre las marcas de tiempo de los registros individua les de la pista de auditoría].	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	La organizac ión recopila los registros de auditoría de [asignación: componentes del sistema definidos por la organización] en un registro de auditoría (lógico o físico) de todo el sistema que se sincroniza con el [asignación: nivel de tolerancia definido por la organización para la relación entre las marcas de tiempo de los registros individua les de la pista de auditoría].	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-12	La organizac ión recopila los registros de auditoría de [asignación: componentes del sistema definidos por la organización] en un registro de auditoría (lógico o físico) de todo el sistema que se sincroniza con el [asignación: nivel de tolerancia definido por la organización para la relación entre las marcas de tiempo de los registros individua les de la pista de auditoría].	wafv2-logging-enab led	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-03	La organización determina cuáles son los tipos de cambios en el sistema que están controlados por la configuración y los documenta.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-08 (02)	La organización mantiene el inventario de los componentes del sistema actualizado, íntegro, completo, preciso y disponible, usando para ello [asignación: mecanismos automatizados definidos por la organización].	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-08 (02)	La organización mantiene el inventario de los componentes del sistema actualizado, íntegro, completo, preciso y disponible, usando para ello [asignación: mecanismos automatizados definidos por la organización].	ec2- -comprobar managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CM-08 (02)	La organización mantiene el inventario de los componentes del sistema actualizado, íntegro, completo, preciso y disponible, usando para ello [asignación: mecanismos automatizados definidos por la organización].	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-02 (05)	La organización establece un plan para continuar con sus objetivos y sus funciones comerciales con un nivel mínimo o nulo de pérdidas en el flujo operativo , y mantiene esa continuidad hasta que se restablezca por completo el sistema en los sitios principal es de procesamiento o almacenamiento.	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	Regla de AWS Config	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	backup-recovery-point-minimum-retention-check	Comprueba que un punto de recuperación no caduque antes de que concluya el período especificado. Las organizaciones establecen objetivos de tiempo y punto de recuperación como parte de la planificación de contingencias. La configuración del sitio de almacenamiento alternativo incluye las instalaciones físicas, así como los sistemas que respaldan las operaciones de recuperación y que garantizan la accesibilidad y la correcta ejecución.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	rds-in-backup-plan	Comprueba si las bases de datos de Amazon Relational Database Service (Amazon RDS) están presentes en los planes de AWS Backup. Las organizaciones establecen objetivos de tiempo y punto de recuperación como parte de la planificación de contingencias. La configuración del sitio de almacenamiento alternativo incluye las instalaciones físicas, así como los sistemas que respaldan las operaciones de recuperación y que garantizan la accesibilidad y la correcta ejecución.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	dynamodb-in-backup-plan	Comprueba si la tabla de Amazon DynamoDB está presente en los planes de AWS Backup. Las organizaciones establecen objetivos de tiempo y punto de recuperación como parte de la planificación de contingencias. La configuración del sitio de almacenamiento alternativo incluye las instalaciones físicas, así como los sistemas que respaldan las operaciones de recuperación y que garantizan la accesibilidad y la correcta ejecución.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operacion es de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperac ión.	ebs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	efs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELB) para poder conservar la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB usa el servicio de escalado automático de aplicaciones de AWS para ajustar de manera automática a la capacidad de rendimiento aprovisionada en respuesta a los patrones de tráfico reales. Esto permite a una tabla o índice secundario global incrementar su capacidad de lectura y escritura aprovisionada para gestionar incrementos repentinos del tráfico sin limitaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando se habilitan las copias de seguridad automáticas, Amazon ElastiCache crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	Regla de AWS Config	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operacion es de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperac ión.	s3- bucket-versioning-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-06 (02)	La organización configura el sitio de almacenamiento alternativo para facilitar las operaciones de recuperación, de acuerdo con los objetivos de tiempo y punto de recuperación.	vpc-vpn-2-tunnels-up	Para cumplir los requisitos de resiliencia, pueden implementarse túneles de Site-to-Site VPN redundantes. Se utilizan dos túneles para garantizar la conectividad en caso de que una de las conexiones de Site-to-Site VPN no esté disponible. Para protegerse frente a la pérdida de conectividad que se produciría si su puerta de enlace de cliente dejara de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN con la Amazon Virtual Private Cloud (Amazon VPC) y la puerta de enlace privada virtual con otro dispositivo de puerta de enlace de cliente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-07 (01)	La organización identifica un sitio de procesamiento alternativo que esté lo suficientemente separado del sitio de procesamiento principal como para reducir la susceptibilidad a las mismas amenazas.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	Regla de AWS Config	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-07 (04)	La organización prepara el sitio de procesamiento alternativo de tal modo que pueda servir como sitio operativo para el desarrollo de las funciones empresariales y los objetivos más importantes.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de copia de seguridad de datos, asegúrese de que su plan de AWS Backup esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer los parámetros requiredFrequencyValue (valor predeterminado de Config: 1), requiredRetentionDays (valor predeterminado de Config: 35) y

ID de control	Descripción del control	Regla de AWS Config	Directrices
			requiredFrequencyUnit (valor predeterminado de Config: days). El valor real debe reflejar los requisitos de su organización.
CP-07 (04)	La organización prepara el sitio de procesamiento alternativo de tal modo que pueda servir como sitio operativo para el desarrollo de las funciones empresariales y los objetivos más importantes.	backup-recovery-point-encrypted	Comprueba si se ha cifrado un punto de recuperación. La preparación del sitio incluye establecer los ajustes de configuración de los sistemas en el sitio de procesamiento alternativo, de acuerdo con los requisitos de dichos ajustes en el sitio principal y estableciendo los suministros esenciales y los procedimientos logísticos que correspondan.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-07 (04)	La organización prepara el sitio de procesamiento alternativo de tal modo que pueda servir como sitio operativo para el desarrollo de las funciones empresariales y los objetivos más importantes.	backup-recovery-point-manual-deletion-disabled	Comprueba si un almacén de copias de seguridad tiene adjunta una política basada en recursos que impide la eliminación de los puntos de recuperación. La preparación del sitio incluye establecer los ajustes de configuración de los sistemas en el sitio de procesamiento alternativo, de acuerdo con los requisitos de dichos ajustes en el sitio principal y estableciendo los suministros esenciales y los procedimientos logísticos que correspondan.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-07 (04)	La organización prepara el sitio de procesamiento alternativo de tal modo que pueda servir como sitio operativo para el desarrollo de las funciones empresariales y los objetivos más importantes.	habilitado para bucket-cross-region-replication s3	Comprueba si ha activado la replicación entre regiones de S3 para los buckets de Amazon S3. La preparación del sitio incluye establecer los ajustes de configuración de los sistemas en el sitio de procesamiento alternativo, de acuerdo con los requisitos de dichos ajustes en el sitio principal y estableciendo los suministros esenciales y los procedimientos logísticos que correspondan.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relacionados con la seguridad] en una instalación independiente o en un contenedor antincendios que no esté junto a la ubicación física del sistema operativo.	backup-recovery-point-minimum-retention-check	Comprueba que un punto de recuperación no caduque antes de que concluya el período especificado. El almacenamiento independiente para la información esencial se aplica a cualquier tipo de información esencial, independientemente del tipo de medio de almacenamiento de seguridad. El software esencial del sistema incluye los sistemas operativos, el middleware, los sistemas de administración de claves criptográficas y los sistemas de detección de intrusiones. La información relacionada con la seguridad incluye los inventarios de los componentes de hardware, software y firmware del sistema. Los sitios de almacenamiento alternativos, como las arquitecturas

ID de control	Descripción del control	Regla de AWS Config	Directrices
			distribuidas geográficamente, funcionan como instalaciones de almacenamiento independientes para las organizaciones. Las organizaciones pueden proporcionar almacenamiento independiente implementando procesos de copia de seguridad automatizados en sitios de almacenamiento alternativos (por ejemplo, centros de datos). La Administración General de Servicios (GSA) establece normas y especificaciones para los contenedores antincendios y de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relaciona dos con la seguridad] en una instalación independiente o en un contenedor antincend ios que no esté junto a la ubicación física del sistema operativo.	aurora-resources-p rotected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relacionados con la seguridad] en una instalación independiente o en un contenedor antincendios que no esté junto a la ubicación física del sistema operativo.	ebs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relacionados con la seguridad] en una instalación independiente o en un contenedor antincendios que no esté junto a la ubicación física del sistema operativo.	efs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relacionados con la seguridad] en una instalación independiente o en un contenedor antincendios que no esté junto a la ubicación física del sistema operativo.	rds-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un plan de AWSBackup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relacionados con la seguridad] en una instalación independiente o en un contenedor antincendios que no esté junto a la ubicación física del sistema operativo.	s3-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relacionados con la seguridad] en una instalación independiente o en un contenedor antincendios que no esté junto a la ubicación física del sistema operativo.	fsx-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus sistemas de archivos de Amazon FSx formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relaciona dos con la seguridad] en una instalación independiente o en un contenedor antincend ios que no esté junto a la ubicación física del sistema operativo.	dynamodb-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relacionados con la seguridad] en una instalación independiente o en un contenedor antincendios que no esté junto a la ubicación física del sistema operativo.	ec2-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (03)	La organización guarda copias de seguridad del [asignación: software de sistema esencial definido por la organización y de otros datos relaciona dos con la seguridad] en una instalación independiente o en un contenedor antincend ios que no esté junto a la ubicación física del sistema operativo.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.
CP-09 (05)	La organización transfiere la informaci ón de copia de seguridad del sistema al sitio de almacenam iento alternativo en un [asignación: período de tiempo y velocidad de transfere ncia definidos por la organización, de acuerdo con los objetivos de tiempo y punto de recuperac ión].	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (05)	La organización transfiere la información de copia de seguridad del sistema al sitio de almacenamiento alternativo en un [asignación: período de tiempo y velocidad de transferencia definidos por la organización, de acuerdo con los objetivos de tiempo y punto de recuperación].	backup-recovery-point-minimum-retention-check	Comprueba que un punto de recuperación no caduque antes de que concluya el período especificado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (05)	La organización transfiere la información de copia de seguridad del sistema al sitio de almacenamiento alternativo en un [asignación: período de tiempo y velocidad de transferencia definidos por la organización, de acuerdo con los objetivos de tiempo y punto de recuperación].	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de copia de seguridad de datos, asegúrese de que su plan de AWS Backup esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer los parámetros requiredFrequencyValue (valor predeterminado de Config: 1), requiredRetentionDays (valor predeterminado de Config: 35) y

ID de control	Descripción del control	Regla de AWS Config	Directrices
			requiredFrequencyUnit (valor predeterminado de Config: days). El valor real debe reflejar los requisitos de su organización.
CP-09 (05)	La organización transfiere la información de copia de seguridad del sistema al sitio de almacenamiento alternativo en un [asignación: período de tiempo y velocidad de transferencia definidos por la organización, de acuerdo con los objetivos de tiempo y punto de recuperación].	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (05)	La organización transfiere la informaci ón de copia de seguridad del sistema al sitio de almacenam iento alternativo en un [asignación: período de tiempo y velocidad de transfere ncia definidos por la organización, de acuerdo con los objetivos de tiempo y punto de recuperac ión].	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	Regla de AWS Config	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-09 (08)	La organización emplea mecanismos criptográficos para evitar la divulgación no autorizada de información de copia de seguridad.	backup-recovery-point-encrypted	La selección de los mecanismos criptográficos se basa en la necesidad de proteger la confidencialidad y la integridad de la información de copia de seguridad. La solidez de los mecanismos seleccionados es proporcional a la categoría de seguridad o a la clasificación de la información. La protección criptográfica se aplica a la información de copia de seguridad del sistema almacenada tanto en las ubicaciones principales como en las alternativas. Las organizaciones que implementan mecanismos criptográficos para proteger la información en reposo también tienen en cuenta soluciones de administración de claves criptográficas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10 (04)	La organización puede restaurar los componentes del sistema dentro de los [asignación: períodos de tiempo de restauración definidos por la organización], a partir de informaci ón cuya integridad está protegida y que está controlada por configuración; dicha información constituy e un estado operativo conocido para los componentes.	backup-recovery-po int-encrypted	Active esta regla para comprobar si se ha cifrado un punto de recuperación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10 (04)	La organización puede restaurar los componentes del sistema dentro de los [asignación: períodos de tiempo de restauración definidos por la organización], a partir de información cuya integridad está protegida y que está controlada por configuración; dicha información constituye un estado operativo conocido para los componentes.	backup-recovery-point-minimum-retention-check	Active esta regla para comprobar que un punto de recuperación no vencerá hasta después del período especificado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10 (04)	La organización puede restaurar los componentes del sistema dentro de los [asignación: períodos de tiempo de restauración definidos por la organización], a partir de informaci ón cuya integridad está protegida y que está controlada por configuración; dicha información constituy e un estado operativo conocido para los componentes.	dynamodb-pitr-enab led	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10 (04)	La organización puede restaurar los componentes del sistema dentro de los [asignación: períodos de tiempo de restauración definidos por la organización], a partir de informaci ón cuya integridad está protegida y que está controlada por configuración; dicha información constituy e un estado operativo conocido para los componentes.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-10 (04)	La organización puede restaurar los componentes del sistema dentro de los [asignación: períodos de tiempo de restauración definidos por la organización], a partir de informaci ón cuya integridad está protegida y que está controlada por configuración; dicha información constituy e un estado operativo conocido para los componentes.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-02 (02)	Implementación de la autenticación multifactorial para acceder a cuentas sin privilegios	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-02 (02)	Implementación de la autenticación multifactorial para acceder a cuentas sin privilegios	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-02 (06)	El sistema de información implementa la autenticación multifactor para el acceso [selección (una o más): local; remoto; por red] a [selección (una o más): cuentas con privilegios; cuentas sin privilegios], de modo que (a) uno de los factores esté suministrado por un dispositivo independiente del sistema que accede y (b) el dispositivo cumpla con los [asignación: requisitos de solidez del mecanismo definidos por la organización].	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-02 (06)	El sistema de información implementa la autenticación multifactor para el acceso [selección (una o más): local; remoto; por red] a [selección (una o más): cuentas con privilegios; cuentas sin privilegios], de modo que (a) uno de los factores esté suministrado por un dispositivo independiente del sistema que accede y (b) el dispositivo cumpla con los [asignación: requisitos de solidez del mecanismo definidos por la organización].	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-02 (08)	El sistema de información implementa mecanismos de autenticación antirreproducción para acceder a [selección (una o más): cuentas con privilegios; cuentas sin privilegios].	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-05 (08)	El sistema de información implementa [asignación: controles de seguridad definidos por la organización] para gestionar los riesgos que se generan cuando hay personas con cuentas en distintos sistemas.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-05 (08)	El sistema de información implementa [asignación: controles de seguridad definidos por la organización] para gestionar los riesgos que se generan cuando hay personas con cuentas en distintos sistemas.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-05 (08)	El sistema de información implementa [asignación: controles de seguridad definidos por la organización] para gestionar los riesgos que se generan cuando hay personas con cuentas en distintos sistemas.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-05 (08)	El sistema de información implementa [asignación: controles de seguridad definidos por la organización] para gestionar los riesgos que se generan cuando hay personas con cuentas en distintos sistemas.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-05 (08)	El sistema de información implementa [asignación: controles de seguridad definidos por la organización] para gestionar los riesgos que se generan cuando hay personas con cuentas en distintos sistemas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-05 (08)	El sistema de información implementa [asignación: controles de seguridad definidos por la organización] para gestionar los riesgos que se generan cuando hay personas con cuentas en distintos sistemas.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios de IAM sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-04 (04)	La organización emplea mecanismos automatizados para correlacionar la información sobre los incidentes y las respuestas individuales a estos, a fin de lograr una perspectiva global de la organización sobre el conocimiento de los incidentes y la respuesta a ellos.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-04 (04)	La organización emplea mecanismos automatizados para correlacionar la información sobre los incidentes y las respuestas individuales a estos, a fin de lograr una perspectiva global de la organización sobre el conocimiento de los incidentes y la respuesta a ellos.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.
IR-04 (04)	La organización emplea mecanismos automatizados para correlacionar la información sobre los incidentes y las respuestas individuales a estos, a fin de lograr una perspectiva global de la organización sobre el conocimiento de los incidentes y la respuesta a ellos.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-04 (04)	La organización emplea mecanismos automatizados para correlacionar la información sobre los incidentes y las respuestas individuales a estos, a fin de lograr una perspectiva global de la organización sobre el conocimiento de los incidentes y la respuesta a ellos.	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IR-04 (04)	La organización emplea mecanismos automatizados para correlacionar la información sobre los incidentes y las respuestas individuales a estos, a fin de lograr una perspectiva global de la organización sobre el conocimiento de los incidentes y la respuesta a ellos.	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.
RA-05	Supervisar y analizar en busca de vulnerabilidades en las aplicaciones alojadas; al encontrar nuevas vulnerabilidades que podrían afectar al sistema, estas se identifican y se genera un informe sobre ellas	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-05	Definir el alcance y la profundidad de la cobertura del análisis de vulnerabilidades.	inspector-lambda-standard-scan-habilitado	Comprueba si el análisis estándar de Lambda con Amazon Inspector V2 está activado en el entorno de una o varias cuentas, a fin de detectar posibles vulnerabilidades de software. La regla es NON_COMPLIANT si el análisis estándar de Lambda no está activado.
RA-05	Definir el alcance y la profundidad de la cobertura del análisis de vulnerabilidades.	inspector-ec2-scan-enabled	Comprueba si el análisis de EC2 de Amazon Inspector V2 está activado en el entorno, de una o varias cuentas, a fin de detectar posibles vulnerabilidades y problemas de accesibilidad de red en las instancias de EC2. La regla es NON_COMPLIANT si el análisis de EC2 no está activado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-05	Definir el alcance y la profundidad de la cobertura del análisis de vulnerabilidades.	inspector-ecr-scan-enabled	Comprueba si el análisis de ECR de Amazon Inspector V2 está activado en el entorno, de una o varias cuentas, a fin de detectar posibles vulnerabilidades en las imágenes de contenedor. La regla es NON_COMPLIANT si el análisis de ECR no está activado.
RA-05 (03)	Definir el alcance y la profundidad de la cobertura del análisis de vulnerabilidades.	inspector-lambda-standard-scan-habilitado	Comprueba si el análisis estándar de Lambda con Amazon Inspector V2 está activado en el entorno de una o varias cuentas, a fin de detectar posibles vulnerabilidades de software. La regla es NON_COMPLIANT si el análisis estándar de Lambda no está activado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-05 (03)	Definir el alcance y la profundidad de la cobertura del análisis de vulnerabilidades.	inspector-ec2-scan-enabled	Comprueba si el análisis de EC2 de Amazon Inspector V2 está activado en el entorno, de una o varias cuentas, a fin de detectar posibles vulnerabilidades y problemas de accesibilidad de red en las instancias de EC2. La regla es NON_COMPLIANT si el análisis de EC2 no está activado.
RA-05 (03)	Definir el alcance y la profundidad de la cobertura del análisis de vulnerabilidades.	inspector-ecr-scan-enabled	Comprueba si el análisis de ECR de Amazon Inspector V2 está activado en el entorno, de una o varias cuentas, a fin de detectar posibles vulnerabilidades en las imágenes de contenedor. La regla es NON_COMPLIANT si el análisis de ECR no está activado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-05 (05)	Implementar la autorización de acceso con privilegios a [asignación: componentes del sistema definidos por la organización] para el análisis de la organización (especifica todos los componentes que admiten la autenticación y todos los análisis).	inspector-ec2-scan-enabled	Comprueba si el análisis de EC2 de Amazon Inspector V2 está activado en el entorno, de una o varias cuentas, a fin de detectar posibles vulnerabilidades y problemas de accesibilidad de red en las instancias de EC2. La regla es NON_COMPLIANT si el análisis de EC2 no está activado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-10	La organización exige que el desarrollador del sistema, el componente del sistema o el servicio del sistema (a) lleven a cabo la administración de la configuración durante [selección (una o más): el diseño; el desarrollo; la implementación; el funcionamiento; la eliminación] del sistema, el componente o el servicio; (b) Documente, administre y controle la integridad de los cambios en [asignación: elementos de la configuración definidos por la organización en el marco de la gestión de la configuración]; c. Implemente únicamente los cambios aprobados por la organización en el sistema, component	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	e o servicio; d. documenten los cambios aprobados en el sistema, el componente o el servicio y los posibles efectos de dichos cambios en la seguridad y la privacidad; y (e) Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-07 (12)	La organización implementa [asignación: mecanismos de protección de límites basados en el alojamiento y definidos por la organización] en los [asignación: componentes de sistema definidos por la organización].	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-07 (20)	Proporcionar la capacidad de aislar dinámicamente [asignación: componentes de sistema definidos por la organización] con respecto a otros componentes del sistema.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-07 (21)	Emplear mecanismos de protección de límites para aislar los [asignación: componentes de sistema definidos por la organización] que sirven de apoyo para [asignación: funciones comerciales u objetivos definidos por la organización].	ec-2 instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Amazon VPC para gestionar correctam ente el acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-07(21)	Emplear mecanismos de protección de límites para aislar los [asignación: componentes de sistema definidos por la organización] que sirven de apoyo para [asignación: funciones comerciales u objetivos definidos por la organización].	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	Regla de AWS Config	Directrices
			deben asignarse a una VPC.
SC-12 (01)	Establecer y administrar claves criptográficas cuando la criptografía se utiliza en el sistema de acuerdo con los siguientes requisitos clave de administración: [asignación: requisitos definidos por la organización para la generación, la distribución, el almacenamiento y la destrucción de claves, así como para el acceso a estas].	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se cifran con una clave maestra de cliente (CMK) propiedad de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	ec-2 ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenciales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	elasticsearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service (OpenSearch Service).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenciales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28 (01)	La organización implementa mecanismos criptográficos para evitar la divulgación y la modificación no autorizadas de la siguiente información en reposo en [asignación: medios o componentes de sistema definidos por la organización]: [asignación: información definida por la organización].	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para los secretos de AWS Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (12)	Alertar [asignación: al personal o los roles definidos por la organización] mediante [asignación: mecanismos automatizados definidos por la organización] cuando existan los siguientes indicios de actividad indebida o inusual con implicaciones de seguridad o privacidad: [asignación: actividades definidas por la organización que desencadenen alertas].	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (20)	Implementar las siguientes tareas adicionales de supervisión de usuarios con privilegios: [asignación: supervisión adicional definida por la organización].	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (20)	Implementar las siguientes tareas adicionales de supervisión de usuarios con privilegios: [asignación: supervisión adicional definida por la organización].	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y que se transmitan a los registros de Amazon CloudWatch para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (20)	Implementar las siguientes tareas adicionales de supervisión de usuarios con privilegios: [asignación: supervisión adicional definida por la organización].	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado. CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin

ID de control	Descripción del control	Regla de AWS Config	Directrices
			necesidad de realizar ninguna acción.
SI-04 (20)	Implementar las siguientes tareas adicionales de supervisión de usuarios con privilegios: [asignación: supervisión adicional definida por la organización].	cloud-trail-cloud-watch-registros habilitados	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (20)	Implementar las siguientes tareas adicionales de supervisión de usuarios con privilegios: [asignación: supervisión adicional definida por la organización].	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (20)	Implementar las siguientes tareas adicionales de supervisión de usuarios con privilegios: [asignación: supervisión adicional definida por la organización].	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
SI-04 (20)	Implementar las siguientes tareas adicionales de supervisión de usuarios con privilegios: [asignación: supervisión adicional definida por la organización].	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (20)	Implementar las siguientes tareas adicionales de supervisión de usuarios con privilegios: [asignación: supervisión adicional definida por la organización].	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (20)	Implementar las siguientes tareas adicionales de supervisión de usuarios con privilegios: [asignación: supervisión adicional definida por la organización].	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (22)	(a) Detectar servicios de red que no hayan sido autorizados o aprobados por [asignación: procesos de aprobación o autorización definidos por la organizac ión]; y (b) [selección (una o más): auditar; alertar a [asignaci ón: personal o roles definidos por la organización]] tras la detección.	securityhub-enabled	(A) AWS Security Hub ayuda a supervisa r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector , Amazon Macie, AWS Identity and Access Managemen t (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (22)	(a) Detectar servicios de red que no hayan sido autorizados o aprobados por [asignación: procesos de aprobación o autorización definidos por la organizac ión]; y (b) [selección (una o más): auditar; alertar a [asignaci ón: personal o roles definidos por la organización]] tras la detección.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-04 (22)	(a) Detectar servicios de red que no hayan sido autorizados o aprobados por [asignación: procesos de aprobación o autorización definidos por la organizac ión]; y (b) [selección (una o más): auditar; alertar a [asignaci ón: personal o roles definidos por la organización]] tras la detección.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-05 (01)	Difundir información sobre alertas y avisos de seguridad en toda la organización mediante [asignación: mecanismos automatizados definidos por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-05 (01)	Difundir información sobre alertas y avisos de seguridad en toda la organización mediante [asignación: mecanismos automatizados definidos por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-07 (02)	Emplear herramientas automatizadas que notifiquen [asignación: al personal o los roles definidos por la organización] al descubrir discrepancias durante la verificación de la integridad.	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-07 (02)	Emplear herramientas automatizadas que notifiquen [asignación: al personal o los roles definidos por la organización] al descubrir discrepancias durante la verificación de la integridad.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-07 (05)	Automáticamente [selección (una o más): apagar el sistema; reiniciar el sistema; implementar [asignación: controles definidos por la organización]] al descubrir infracciones de integridad.	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-07 (05)	Automáticamente [selección (una o más): apagar el sistema; reiniciar el sistema; implementar [asignación: controles definidos por la organización]] al descubrir infracciones de integridad.	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
SI-07 (15)	Implementar mecanismos criptográficos para autenticar los siguientes componentes de software o firmware antes de la instalación: [asignación: componentes de software o firmware definidos por la organización].	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-07 (15)	Implementar mecanismos criptográficos para autenticar los siguientes componentes de software o firmware antes de la instalación: [asignación: componentes de software o firmware definidos por la organización].	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida y compruebe que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (Valor de las prácticas recomendadas de seguridad básica de AWS: 90). El valor real debe reflejar las políticas de su organización.

Plantilla

La plantilla está disponible en GitHub: Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 2).

Prácticas operativas recomendadas para FFIEC

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los dominios de la herramienta de evaluación de ciberseguridad del Consejo Federal de Examen de Instituciones Financieras (FFIEC) y las reglas de AWS Config administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de la herramienta de evaluación de ciberseguridad de la FFIEC. El control de la herramienta de evaluación de ciberseguridad del FFIEC puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.G.IT.B.1	Se mantiene un inventario de los activos de la organización (por ejemplo, hardware, software, datos y sistemas alojados externamente).	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			detalles sobre su entorno.
D1.G.IT.B.1	Se mantiene un inventario de los activos de la organización (por ejemplo, hardware, software, datos y sistemas alojados externamente).	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.G.IT.B.1	Se mantiene un inventario de los activos de la organización (por ejemplo, hardware, software, datos y sistemas alojados externamente).	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.G.IT.B.1	Se mantiene un inventario de los activos de la organización (por ejemplo, hardware, software, datos y sistemas alojados externamente).	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.Rm.B.1	Dentro de la institución existen roles de gestión de riesgos de seguridad de la información y de continuidad del negocio.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.RM.RA.B.2	La evaluación de riesgos identifica los sistemas basados en internet y las transacciones de alto riesgo que requieren controles de autentica ción adicionales.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
D1.RM.RA.B.2	La evaluación de riesgos identifica los sistemas basados en internet y las transacciones de alto riesgo que requieren controles de autentica ción adicionales.	annual-risk-assess ment-performed (verificación de procesos)	Realice una evaluació n anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determina r la probabilidad y el impacto de los riesgos y and/or vulnerabi lidades identificados que afectan a una organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.TC.Tr.B.2	La formación anual sobre seguridad de la información incluye la respuesta ante incidentes, las ciberamenazas actuales (por ejemplo, la suplantación de identidad, el spear phishing, la ingenierí a social y la seguridad móvil) y las cuestione s emergentes.	security-awareness -program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infraccio nes o incidentes de seguridad.
D2.IS.Is.B.1	Las amenazas a la seguridad de la información se recopilan y comparten con el personal interno correspon diente.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.IS.Is.B.1	Las amenazas a la seguridad de la información se recopilan y comparten con el personal interno correspon diente.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.IS.Is.B.1	Las amenazas a la seguridad de la información se recopilan y comparten con el personal interno correspon diente.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	s3- bucket-default-loc k-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
D2.MA.Ma.B.1	Los registros de auditoría y otros registros de eventos de seguridad se revisan y conservan de forma segura.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.MA.Ma.B.2	Los registros de eventos informáticos se utilizan para las investigaciones después de un evento.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.TI.Ti.B.1	La institución pertenece, o está suscrita, a fuentes de intercambio de información sobre amenazas y vulnerabilidades que proporcionan información sobre las amenazas (por ejemplo, FS-ISAC, US-CERT).	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.TI.Ti.B.1	La institución pertenece, o está suscrita, a fuentes de intercambio de información sobre amenazas y vulnerabilidades que proporcionan información sobre las amenazas (por ejemplo, FS-ISAC, US-CERT).	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.TI.Ti.B.2	La información sobre amenazas se usa para monitorear las amenazas y vulnerabilidades.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.TI.Ti.B.2	La información sobre amenazas se usa para monitorear las amenazas y vulnerabilidades.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.TI.Ti.B.2	La información sobre amenazas se usa para monitorear las amenazas y vulnerabilidades.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.TI.Ti.B.3	La información sobre amenazas se utiliza para mejorar la gestión y los controles internos de los riesgos.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D2.TI.Ti.B.3	La información sobre amenazas se utiliza para mejorar la gestión y los controles internos de los riesgos.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.CC.PM.B.1	Se implementa un programa de administración de parches que garantiza que los parches de software y firmware se apliquen de manera oportuna.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.CC.PM.B.1	Se implementa un programa de administración de parches que garantiza que los parches de software y firmware se apliquen de manera oportuna.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.CC.PM.B.1	Se implementa un programa de administración de parches que garantiza que los parches de software y firmware se apliquen de manera oportuna.	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.CC.PM.B.1	Se implementa un programa de administración de parches que garantiza que los parches de software y firmware se apliquen de manera oportuna.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
D3.CC.PM.B.3	Se revisan los informes de administración de parches y se muestran los parches de seguridad que faltan.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.CC.PM.B.3	Se revisan los informes de administración de parches y se muestran los parches de seguridad que faltan.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.CC.PM.B.3	Se revisan los informes de administración de parches y se muestran los parches de seguridad que faltan.	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.CC.PM.B.3	Se revisan los informes de administración de parches y se muestran los parches de seguridad que faltan.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
D3.DC.An.B.1	La institución es capaz de detectar actividades anómalas mediante el monitoreo en todo el entorno.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.1	La institución es capaz de detectar actividades anómalas mediante el monitoreo en todo el entorno.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.1	La institución es capaz de detectar actividades anómalas mediante el monitoreo en todo el entorno.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.2	Se monitorean y revisan las transacciones de los clientes que generan alertas de actividad anómala.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.2	Se monitorean y revisan las transacciones de los clientes que generan alertas de actividad anómala.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.3	Los registros de acceso físico y and/or lógico se revisan después de los eventos.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.3	Los registros de acceso físico y and/or lógico se revisan después de los eventos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.3	Los registros de acceso físico y and/or lógico se revisan después de los eventos.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.3	Los registros de acceso físico y and/or lógico se revisan después de los eventos.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.3	Los registros de acceso and/or lógico físico se revisan después de los eventos.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.3	Los registros de acceso físico y and/or lógico se revisan después de los eventos.	cloud-trail-cloud-watch-habilitados para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
D3.DC.An.B.3	Los registros de acceso físico y and/or lógico se revisan después de los eventos.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.3	Los registros de acceso físico y and/or lógico se revisan después de los eventos.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.3	Los registros de acceso and/or lógico físico se revisan después de los eventos.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
D3.DC.An.B.3	Los registros de acceso and/or lógico físico se revisan después de los eventos.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.3	Los registros de acceso físico y and/or lógico se revisan después de los eventos.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
D3.DC.An.B.4	Se monitorea el acceso de terceros a los sistemas esenciales para detectar actividad es no autorizadas o inusuales.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.5	Se monitorean los privilegios elevados.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.An.B.5	Se monitorean los privilegios elevados.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
D3.DC.Ev.B.1	Se establece una línea base de actividad de red normal.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultane idad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.1	Se establece una línea base de actividad de red normal.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
D3.DC.Ev.B.1	Se establece una línea base de actividad de red normal.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.1	Se establece una línea base de actividad de red normal.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.1	Se establece una línea base de actividad de red normal.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.1	Se establece una línea base de actividad de red normal.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.1	Se establece una línea base de actividad de red normal.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.1	Se establece una línea base de actividad de red normal.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.1	Se establece una línea base de actividad de red normal.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.2	Existen mecanismos (por ejemplo, alertas de antivirus, alertas de evento de registro) para informar a la dirección sobre posibles ataques.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.3	Existen procesos para monitorea r la presencia de usuarios, dispositivos, conexiones y software no autorizados.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.3	Existen procesos para monitorea r la presencia de usuarios, dispositivos, conexiones y software no autorizados.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.3	Existen procesos para monitorea r la presencia de usuarios, dispositivos, conexiones y software no autorizados.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Ev.B.3	Existen procesos para monitorea r la presencia de usuarios, dispositivos, conexiones y software no autorizados.	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Th.B.1	Las pruebas independientes (incluidas las pruebas de penetración y el análisis de vulnerabilidades) se llevan a cabo de acuerdo con la evaluación de riesgos para los sistemas externos y la red interna.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Th.B.1	Las pruebas independientes (incluidas las pruebas de penetración y el análisis de vulnerabilidades) se llevan a cabo de acuerdo con la evaluación de riesgos para los sistemas externos y la red interna.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.DC.Th.B.1	Las pruebas independientes (incluidas las pruebas de penetración y el análisis de vulnerabilidades) se llevan a cabo de acuerdo con la evaluación de riesgos para los sistemas externos y la red interna.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsabilidades laborales y de conformidad con los principios de privilegio mínimo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsabilidades laborales y de conformidad con los principios de privilegio mínimo.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsab ilidades laborales y de conformidad con los principios de privilegio mínimo.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsabilidades laborales y de conformidad con los principios de privilegio mínimo.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsab ilidades laborales y de conformidad con los principios de privilegio mínimo.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsab ilidades laborales y de conformidad con los principios de privilegio mínimo.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsab ilidades laborales y de conformidad con los principios de privilegio mínimo.	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsab ilidades laborales y de conformidad con los principios de privilegio mínimo.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsab ilidades laborales y de conformidad con los principios de privilegio mínimo.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsab ilidades laborales y de conformidad con los principios de privilegio mínimo.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEncryptFrom)

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			. Los valores reales deben reflejar las políticas de su organización.
D3.PC.Am.B.1	El acceso del personal a los sistemas y a los datos confidenciales se concede en función de las responsabilidades laborales y de conformidad con los principios de privilegio mínimo.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.10	Los entornos de producción y no producción están divididos para evitar el acceso no autorizado o los cambios en los activos de información. (*N/A si no existe un entorno de producción en la institución o en un tercero de la institución).	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
D3.PC.Am.B.10	Los entornos de producción y no producción están divididos para evitar el acceso no autorizad o o los cambios en los activos de información. (*N/A si no existe un entorno de producción en la institución o en un tercero de la instituci ón).	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube aseguránd ose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.10	Los entornos de producción y no producción están divididos para evitar el acceso no autorizad o o los cambios en los activos de información. (*N/A si no existe un entorno de producción en la institución o en un tercero de la instituci ón).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.10	Los entornos de producción y no producción están divididos para evitar el acceso no autorizado o los cambios en los activos de información. (*N/A si no existe un entorno de producción en la institución o en un tercero de la institución).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	s3- -habilitado bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
D3.PC.Am.B.12	Se cifran todas las contraseñas tanto en almacenamiento como en tránsito.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.13	Los datos confidenciales se cifran cuando se transmiten a través de redes públicas o no fiables (por ejemplo, Internet).	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
D3.PC.Am.B.13	Los datos confidenciales se cifran cuando se transmiten a través de redes públicas o no fiables (por ejemplo, Internet).	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.13	Los datos confidenciales se cifran cuando se transmiten a través de redes públicas o no fiables (por ejemplo, Internet).	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
D3.PC.Am.B.13	Los datos confidenciales se cifran cuando se transmiten a través de redes públicas o no fiables (por ejemplo, Internet).	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.13	Los datos confidenciales se cifran cuando se transmiten a través de redes públicas o no fiables (por ejemplo, Internet).	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
D3.PC.Am.B.13	Los datos confidenciales se cifran cuando se transmiten a través de redes públicas o no fiables (por ejemplo, Internet).	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.13	Los datos confidenciales se cifran cuando se transmiten a través de redes públicas o no fiables (por ejemplo, Internet).	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.15	El acceso remoto a los sistemas esenciales por parte del personal, contratistas y terceros se realiza mediante conexiones cifradas y autenticación multifactor.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.15	El acceso remoto a los sistemas esenciales por parte del personal, contratistas y terceros se realiza mediante conexiones cifradas y autenticación multifactor.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.15	El acceso remoto a los sistemas esenciales por parte del personal, contratistas y terceros se realiza mediante conexiones cifradas y autenticación multifactor.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.15	El acceso remoto a los sistemas esenciales por parte del personal, contratistas y terceros se realiza mediante conexiones cifradas y autenticación multifactor.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.15	El acceso remoto a los sistemas esenciales por parte del personal, contratistas y terceros se realiza mediante conexiones cifradas y autenticación multifactor.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
D3.PC.Am.B.15	El acceso remoto a los sistemas esenciales por parte del personal, contratistas y terceros se realiza mediante conexiones cifradas y autenticación multifactor.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.15	El acceso remoto a los sistemas esenciales por parte del personal, contratistas y terceros se realiza mediante conexiones cifradas y autenticación multifactor.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.16	Existen controles administrativos, físicos o técnicos para evitar que los usuarios sin responsabilidades administrativas instalen software no autorizado.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.16	Existen controles administrativos, físicos o técnicos para evitar que los usuarios sin responsabilidades administrativas instalen software no autorizado.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.16	Existen controles administrativos, físicos o técnicos para evitar que los usuarios sin responsabilidades administrativas instalen software no autorizado.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
D3.PC.Am.B.16	Existen controles administrativos, físicos o técnicos para evitar que los usuarios sin responsabilidades administrativas instalen software no autorizado.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.2	El acceso del personal a los sistemas y a los datos confidenciales permite la separación de funciones.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.2	El acceso del personal a los sistemas y a los datos confidenciales permite la separación de funciones.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
D3.PC.Am.B.2	El acceso del personal a los sistemas y a los datos confidenciales permite la separación de funciones.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.3	Los privilegios elevados (por ejemplo, los privilegios de administrador) son limitados y se controlan de forma estricta (por ejemplo, se asignan a personas, no se comparten y requieren controles de contraseña más estrictos).	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.3	Los privilegios elevados (por ejemplo, los privilegios de administrador) son limitados y se controlan de forma estricta (por ejemplo, se asignan a personas, no se comparten y requieren controles de contraseña más estrictos).	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.3	Los privilegios elevados (por ejemplo, los privilegios de administrador) son limitados y se controlan de forma estricta (por ejemplo, se asignan a personas, no se comparten y requieren controles de contraseña más estrictos).	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.3	Los privilegios elevados (por ejemplo, los privilegios de administrador) son limitados y se controlan de forma estricta (por ejemplo, se asignan a personas, no se comparten y requieren controles de contraseña más estrictos).	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.3	Los privilegios elevados (por ejemplo, los privilegios de administrador) son limitados y se controlan de forma estricta (por ejemplo, se asignan a personas, no se comparten y requieren controles de contraseña más estrictos).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.3	Los privilegios elevados (por ejemplo, los privilegios de administrador) son limitados y se controlan de forma estricta (por ejemplo, se asignan a personas, no se comparten y requieren controles de contraseña más estrictos).	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
D3.PC.Am.B.6	La identificación y la autenticación son obligatorias y se administran para acceder a los sistemas, las aplicaciones y el hardware.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.7	Los controles de acceso incluyen complejidad de las contraseñas, límites de intentos y de reutilización de contraseñas.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Am.B.8	Todas las contraseñas predeterminadas y las cuentas predeterminadas innecesarias se cambian antes de la implementación del sistema.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.1	Se utilizan herramientas de defensa perimetral de la red (por ejemplo, un enrutador perimetral y un firewall).	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.2	Los sistemas a los que se accede desde internet o desde terceros están protegidos por firewalls u otros dispositivos similares.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.2	Los sistemas a los que se accede desde internet o desde terceros están protegidos por firewalls u otros dispositivos similares.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.2	Los sistemas a los que se accede desde internet o desde terceros están protegidos por firewalls u otros dispositivos similares.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.2	Los sistemas a los que se accede desde internet o desde terceros están protegidos por firewalls u otros dispositivos similares.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.2	Los sistemas a los que se accede desde internet o desde terceros están protegidos por firewalls u otros dispositivos similares.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.2	Los sistemas a los que se accede desde internet o desde terceros están protegidos por firewalls u otros dispositivos similares.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.3	Todos los puertos están monitorizados.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.3	Todos los puertos están monitorizados.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
D3.PC.IM.B.3	Todos los puertos están monitorizados.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.3	Todos los puertos están monitorizados.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.3	Todos los puertos están monitorizados.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.3	Todos los puertos están monitorizados.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.5	Las configuraciones de los sistemas (para servidores, equipos de sobremesa, enrutadores, etc.) siguen los estándares del sector que se deben cumplir.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.5	Las configuraciones de los sistemas (para servidores, equipos de sobremesa, enrutadores, etc.) siguen los estándares del sector que se deben cumplir.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.5	Las configuraciones de los sistemas (para servidores, equipos de sobremesa, enrutadores, etc.) siguen los estándares del sector que se deben cumplir.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.6	Los puertos, los roles, los protocolos y los servicios están prohibidos si ya no se necesitan para fines empresariales.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.6	Los puertos, los roles, los protocolos y los servicios están prohibidos si ya no se necesitan para fines empresariales.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.6	Los puertos, los roles, los protocolos y los servicios están prohibidos si ya no se necesitan para fines empresariales.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.IM.B.6	Los puertos, los roles, los protocolos y los servicios están prohibidos si ya no se necesitan para fines empresariales.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.7	El acceso para realizar cambios en las configuraciones de los sistemas (incluidas las máquinas virtuales y los hipervisores) se controla y monitorea.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.7	El acceso para realizar cambios en las configuraciones de los sistemas (incluidas las máquinas virtuales y los hipervisores) se controla y monitorea.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.7	El acceso para realizar cambios en las configuraciones de los sistemas (incluidas las máquinas virtuales y los hipervisores) se controla y monitorea.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.7	El acceso para realizar cambios en las configuraciones de los sistemas (incluidas las máquinas virtuales y los hipervisores) se controla y monitorea.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.7	El acceso para realizar cambios en las configuraciones de los sistemas (incluidas las máquinas virtuales y los hipervisores) se controla y monitorea.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Im.B.7	El acceso para realizar cambios en las configuraciones de los sistemas (incluidas las máquinas virtuales y los hipervisores) se controla y monitorea.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
D3.PC.Im.B.7	El acceso para realizar cambios en las configuraciones de los sistemas (incluidas las máquinas virtuales y los hipervisores) se controla y monitorea.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Se.B.1	Los desarrolladores que trabajan para la institución siguen prácticas seguras de codificación de programas, como parte de un ciclo de vida de desarrollo del sistema (SDLC), que cumplen con los estándares del sector.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D3.PC.Se.B.1	Los desarrolladores que trabajan para la institución siguen prácticas seguras de codificación de programas, como parte de un ciclo de vida de desarrollo del sistema (SDLC), que cumplen con los estándares del sector.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D4.C.Co.B.2	La institución se asegura de que las conexiones de terceros estén autorizadas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D4.C.Co.B.2	La institución se asegura de que las conexiones de terceros estén autorizadas.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D4.C.Co.B.2	La institución se asegura de que las conexiones de terceros estén autorizadas.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D4.C.Co.B.2	La institución se asegura de que las conexiones de terceros estén autorizadas.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.1	Los parámetros de alerta se establecen para detectar incidentes de seguridad de la información que impulsan acciones de mitigación.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.1	Los parámetros de alerta se establecen para detectar incidentes de seguridad de la información que impulsan acciones de mitigación.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.1	Los parámetros de alerta se establecen para detectar incidentes de seguridad de la información que impulsan acciones de mitigación.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
D5.DR.De.B.2	Los informes de rendimiento del sistema contienen información que se puede utilizar como indicador de riesgo para detectar incidentes de seguridad de la información.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.2	Los informes de rendimiento del sistema contienen información que se puede utilizar como indicador de riesgo para detectar incidentes de seguridad de la información.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	cloud-trail-cloud-watch-registros activados	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.DR.De.B.3	Existen herramientas y procesos para detectar, alertar y activar el programa de respuesta ante incidentes.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.ER.Es.B.4	Los incidentes se clasifican, registran y rastrean.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.
D5.IR.Pl.B.1	La institución ha documentado cómo reaccionará y responderá a los ciberincidentes.	response-plan-exists-maintained (verificación de procesos)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresari al, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresari al, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresari al, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresari al, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresarial, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D5.IR.PI.B.6	La institución planea utilizar programas de continuidad empresari al, recuperación de desastres y copia de seguridad de datos para recuperar las operaciones tras un incidente.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para la FFIEC.

Catálogo de criterios de cumplimiento de las prácticas recomendadas operativas para la computación en la nube en Alemania (C5)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear comprobaciones de control de seguridad, operativas o de optimización de costos mediante reglas de AWS Config administradas o personalizadas y acciones correctivas de AWS Config. Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de asignación entre el Catálogo de criterios de cumplimiento de la computación en la nube de Alemania (C5) y las reglas de AWS Config administradas. Cada regla de Config se aplica a un recurso de AWS específico que está relacionado con uno o más controles C5 de Alemania. Un control C5 de Alemania puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Regla de AWS Config	Directrices
COS-01	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Una WAF ayuda a proteger sus aplicaciones web o API frente a las vulnerabi lidades comunes de la web. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
COS-01	api-gw-associated-with-waf	AWS WAF permite configura r un conjunto de reglas (denominadas lista de control

ID de control	Regla de AWS Config	Directrices
		de acceso web (ACL web) que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personali zables que defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
COS-01	waf-regional-rule-not-empty	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencade nar un comportamiento no deseado.
COS-01	waf-regional-rulegroup-not-empty	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportam iento no deseado.
COS-01	waf-regional-webacl-not-empty	Una ACL web asociada a un AWS WAF puede contener una colección de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.

ID de control	Regla de AWS Config	Directrices
COS-01	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.
COS-03	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicaciones web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Regla de AWS Config	Directrices
COS-03	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicaci ón de DMS. Las instancia s de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
COS-03	ebs-snapshot-public-restora ble-check	Administre el acceso a la nube de AWS de manera que se garantice que las instantán eas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
COS-03	ec2-instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Regla de AWS Config	Directrices
COS-03	ec2-instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	Regla de AWS Config	Directrices
COS-03	elasticsearch-in-vpc-only	Gestione el acceso a la nube de AWS de manera que se garantice que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch Service dentro de una Amazon VPC garantiza una comunicac ión segura entre OpenSearc h Service y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de Internet, un dispositivo NAT o una conexión de VPN.

ID de control	Regla de AWS Config	Directrices
COS-03	opensearch-in-vpc-only	Gestione el acceso a la nube de AWS de manera que se garantice que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC garantiza una comunicac ión segura entre Amazon OpenSearch Service y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN.
COS-03	emr-master-no-public-ip	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Regla de AWS Config	Directrices
COS-03	internet-gateway-authorized-vpc-only	Gestione el acceso a recursos en la nube de AWS de manera que garantice que las puertas de enlace de Internet solo se conecten a la Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
COS-03	lambda-function-public-access-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Regla de AWS Config	Directrices
COS-03	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	Regla de AWS Config	Directrices
COS-03	rds-instance-public-access-check	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.
COS-03	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Regla de AWS Config	Directrices
COS-03	redshift-cluster-public-access-check	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
COS-03	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	Regla de AWS Config	Directrices
COS-03	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Regla de AWS Config	Directrices
COS-03	s3-account-level-public-access-blocks-periodic	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterminado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
COS-03	sagemaker-notebook-no-direct-internet-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
COS-03	vpc-default-security-group-closed	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Regla de AWS Config	Directrices
COS-03	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
COS-03	alb-http-drop-invalid-header-enabled	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Regla de AWS Config	Directrices
COS-05	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
COS-05	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Regla de AWS Config	Directrices
COS-05	root-account-hardware-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.
COS-05	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.

ID de control	Regla de AWS Config	Directrices
COS-05	ec2-instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
COS-05	emr-master-no-public-ip	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Regla de AWS Config	Directrices
COS-05	rds-instance-public-access-check	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.
COS-05	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Regla de AWS Config	Directrices
COS-05	redshift-cluster-public-access-check	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
COS-05	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	Regla de AWS Config	Directrices
COS-05	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
COS-05	vpc-default-security-group-closed	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Regla de AWS Config	Directrices
COS-05	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
CRY-02	alb-http-to-https-redirection-check	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Regla de AWS Config	Directrices
CRY-02	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Regla de AWS Config	Directrices
CRY-02	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La política de seguridad predeterminada es ELBSecurityPolicy-TLS-1-2-2017-0. El valor real debe reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
CRY-02	opensearch-https-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, asegúrese de que HTTPS esté activado para las conexiones en sus dominios de Amazon OpenSearch Service.
CRY-02	elasticsearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicac iones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CRY-02	elb-tls-https-listeners-only	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Regla de AWS Config	Directrices
CRY-02	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CRY-02	s3-bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CRY-02	opensearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Regla de AWS Config	Directrices
CRY-03	api-gw-cache-enabled-and-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
CRY-03	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
CRY-03	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.
CRY-03	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Regla de AWS Config	Directrices
CRY-03	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para los secretos de AWS Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
CRY-03	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se cifran con una clave maestra de cliente (CMK) propiedad de AWS.

ID de control	Regla de AWS Config	Directrices
CRY-03	ebs-snapshot-public-restorable-check	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
CRY-03	ec2-ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CRY-03	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Regla de AWS Config	Directrices
CRY-03	elasticsearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearc h Service (OpenSearch Service).
CRY-03	opensearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service.
CRY-03	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
CRY-03	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Regla de AWS Config	Directrices
CRY-03	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para sus artefactos de AWS CodeBuild.
CRY-03	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Regla de AWS Config	Directrices
CRY-03	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEn abled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.
CRY-03	s3-default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Regla de AWS Config	Directrices
CRY-03	sagemaker-endpoint-configuration-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenciales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.
CRY-03	sagemaker-notebook-instance-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenciales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Regla de AWS Config	Directrices
CRY-03	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
CRY-04	cmk-backing-key-rotation-enabled	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
DEV-07	cloud-trail-cloud-watch-logs-enabled	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su Cuenta de AWS.

ID de control	Regla de AWS Config	Directrices
DEV-07	codebuild-project-logging-enabled	Asegúrese de que el registro de proyectos de AWS CodeBuild esté habilitado para que los registros de salida de compilación se envíen a Amazon CloudWatch o Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.
DEV-07	s3-bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Regla de AWS Config	Directrices
DEV-07	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las Cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.
DEV-07	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la Cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Regla de AWS Config	Directrices
DEV-07	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado . CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Regla de AWS Config	Directrices
IDM-01	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
IDM-01	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	Regla de AWS Config	Directrices
IDM-01	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de

ID de control	Regla de AWS Config	Directrices
		seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñ as de IAM. Los valores reales deben reflejar las políticas de su organización.
IDM-01	iam-root-access-key-check	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de Cuentas de AWS basadas en roles para ayudar a incorpora r el principio de funcionalidad mínima.

ID de control	Regla de AWS Config	Directrices
IDM-01	iam-user-group-membership-check	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
IDM-01	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Regla de AWS Config	Directrices
IDM-01	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabili tarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsage Age (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
IDM-01	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
IDM-01	root-account-hardware-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.

ID de control	Regla de AWS Config	Directrices
IDM-01	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.
IDM-01	secretsmanager-rotation-enabled-check	Esta regla garantiza que los secretos de AWS Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Regla de AWS Config	Directrices
IDM-01	secretsmanager-scheduled-rotation-success-check	Esta regla garantiza que los secretos de AWS Secrets Manager se distribuyan correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
IDM-01	iam-group-has-users-check	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y separación de funciones con permisos y autorizaciones de acceso al garantizar que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegi os mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Regla de AWS Config	Directrices
IDM-01	iam-user-no-policies-check	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
IDM-01	codebuild-project-envvar-awscred-check	Asegúrese de que las credenciales de autenticación AWS_ACCESS_KEY_ID y AWS_SECRET_ACCESS_KEY no existan en los entornos de proyecto de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Regla de AWS Config	Directrices
IDM-01	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.
IDM-01	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Regla de AWS Config	Directrices
IDM-01	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.
IDM-01	efs-access-point-enforce-root-directory	La aplicación de un directori o raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

ID de control	Regla de AWS Config	Directrices
IDM-01	efs-access-point-enforce-user-identity	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en el Amazon Elastic File System (Amazon EFS). Cuando está habilitada, Amazon EFS reemplaza los ID de usuario y grupo del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario obligatoria.
IDM-01	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Regla de AWS Config	Directrices
IDM-01	opensearch-access-control-enabled	Asegúrese de habilitar el control de acceso detallado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con privilegio mínimo a los dominios de Amazon OpenSearch Service. Permite el control de acceso al dominio basado en roles, así como la seguridad en el nivel de índices, documentos y campos, la compatibilidad con los paneles de OpenSearch Service, la tenencia múltiple y la autenticación básica HTTP para OpenSearch Service y Kibana.

ID de control	Regla de AWS Config	Directrices
IDM-01	rds-instance-iam-authentication-enabled	Asegúrese de que la autenticación de AWS Identity and Access Management (IAM) esté habilitada en las instancias de Amazon Relational Database Service (Amazon RDS) para controlar el acceso a los sistemas y activos. De esta manera se fuerza el cifrado del tráfico de red hacia y desde la base de datos mediante la capa de sockets seguros (SSL). No es necesario almacenar credenciales de usuario en la base de datos, ya que la autenticación se administra de forma externa.

ID de control	Regla de AWS Config	Directrices
IDM-01	s3-bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACL) se utilizan para el control de acceso en los buckets de Amazon S3. Las ACL son mecanismos de control de acceso heredados para buckets de Amazon S3 que sean anteriores a AWS Identity and Access Management (IAM). En lugar de las ACL, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Regla de AWS Config	Directrices
IDM-03	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabili tarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsage Age (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.
IDM-03	secretsmanager-secret-unused	Si existen credenciales no utilizadas en AWS Secrets Manager, debe deshabili tarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedForDays (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organizac ión.

ID de control	Regla de AWS Config	Directrices
IDM-08	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de

ID de control	Regla de AWS Config	Directrices
		seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñ as de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
CRY-01	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de

ID de control	Regla de AWS Config	Directrices
		seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñ as de IAM. Los valores reales deben reflejar las políticas de su organización.
IDM-09	iam-user-mfa-enabled	Active esta regla para restringi r el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autentica ción multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidente s de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Regla de AWS Config	Directrices
IDM-09	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
IDM-09	root-account-hardware-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.

ID de control	Regla de AWS Config	Directrices
IDM-09	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.
OPS-01	clb-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantizar una alta disponibilidad, asegúrese de que su ELB tenga instancias registradas de varias zonas de disponibilidad.

ID de control	Regla de AWS Config	Directrices
OPS-01	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantizar una alta disponibilidad, asegúrese de que su ELB tenga instancias registradas de varias zonas de disponibilidad.
OPS-01	lambda-vpc-multi-az-check	Si la función de AWS Lambda está configurada para conectarse a una nube privada virtual (VPC) de su cuenta, implemente la función de AWS Lambda en al menos dos zonas de disponibilidad diferentes para asegurars e de que sea la función que está disponible para procesar eventos en caso de una interrupción del servicio en una sola zona.

ID de control	Regla de AWS Config	Directrices
OPS-01	rds-cluster-multi-az-enabled	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Regla de AWS Config	Directrices
OPS-01	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Regla de AWS Config	Directrices
OPS-01	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB usa el servicio de escalado automático de aplicaciones de AWS para ajustar de manera automática la capacidad de rendimiento aprovisionada en respuesta a los patrones de tráfico reales. Esto permite a una tabla o índice secundario global incrementar su capacidad de lectura y escritura aprovisionada para gestionar incrementos repentinos del tráfico sin limitaciones.
OPS-01	elb-cross-zone-load-balancing-enabled	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELB) para poder conservar la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Regla de AWS Config	Directrices
OPS-01	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de actividad de lectura y escritura que puede admitir cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar de forma opcional los parámetros accountRCUThresholdPercentage (valor predeterminado de Config: 80) y accountWCUThresholdPercentage (valor predeterminado de Config: 80). Los valores reales deben reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
OPS-02	clb-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantizar una alta disponibilidad, asegúrese de que su ELB tenga instancias registradas de varias zonas de disponibilidad.
OPS-02	autoscaling-group-elb-healt hcheck-required	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibi lidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Regla de AWS Config	Directrices
OPS-02	beanstalk-enhanced-health-reporting-enabled	Los informes de estado mejorados de AWS Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.
OPS-02	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuye automáticamente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibilidad. Para garantizar una alta disponibilidad, asegúrese de que su ELB tenga instancias registradas de varias zonas de disponibilidad.

ID de control	Regla de AWS Config	Directrices
OPS-02	lambda-vpc-multi-az-check	Si la función de AWS Lambda está configurada para conectarse a una nube privada virtual (VPC) de su cuenta, implemente la función de AWS Lambda en al menos dos zonas de disponibilidad diferentes para asegurars e de que sea la función que está disponible para procesar eventos en caso de una interrupción del servicio en una sola zona.

ID de control	Regla de AWS Config	Directrices
OPS-02	rds-cluster-multi-az-enabled	Los clústeres de Amazon Relational Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenados. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Regla de AWS Config	Directrices
OPS-02	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Regla de AWS Config	Directrices
OPS-02	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB usa el servicio de escalado automático de aplicaciones de AWS para ajustar de manera automática la capacidad de rendimiento aprovisionada en respuesta a los patrones de tráfico reales. Esto permite a una tabla o índice secundario global incrementar su capacidad de lectura y escritura aprovisionada para gestionar incrementos repentinos del tráfico sin limitaciones.
OPS-02	elb-cross-zone-load-balancing-enabled	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELB) para poder conservar la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Regla de AWS Config	Directrices
OPS-02	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de actividad de lectura y escritura que puede admitir cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar de forma opcional los parámetros accountRCUThresholdPercentage (valor predeterminado de Config: 80) y accountWCUThresholdPercentage (valor predeterminado de Config: 80). Los valores reales deben reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
OPS-07	aurora-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Regla de AWS Config	Directrices
OPS-07	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de copia de seguridad de datos, asegúrese de que su plan de AWS Backup esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad . Esta regla le permite establecer los parámetros requiredFrequencyValue (valor predeterminado de Config: 1), requiredRetentionDays (valor predeterminado de Config: 35) y requiredFrequencyUnit (valor predeterminado de Config: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Regla de AWS Config	Directrices
OPS-07	backup-recovery-point-manual-deletion-disabled	Asegúrese de que los puntos de recuperación de AWS Backup tengan adjunta una política basada en los recursos que impida eliminar los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.
OPS-07	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Regla de AWS Config	Directrices
OPS-07	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) requiere al menos tres nodos de datos para garantiza r la alta disponibilidad y la tolerancia a errores. La implementación de un dominio de OpenSearch Service con al menos tres nodos de datos garantiza las operaciones del clúster en caso de que un nodo falle.

ID de control	Regla de AWS Config	Directrices
OPS-07	backup-recovery-point-minimum-retention-check	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus puntos de recuperación de AWS Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (valor predeterminado de Config: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Regla de AWS Config	Directrices
OPS-07	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Regla de AWS Config	Directrices
OPS-07	dynamodb-in-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus tablas de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Regla de AWS Config	Directrices
OPS-07	ebs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Regla de AWS Config	Directrices
OPS-07	ec2-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Regla de AWS Config	Directrices
OPS-07	efs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Regla de AWS Config	Directrices
OPS-07	elasticache-redis-cluster-automatic-backup-check	Cuando se habilitan las copias de seguridad automáticas, Amazon ElastiCache crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Regla de AWS Config	Directrices
OPS-07	fsx-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus sistemas de archivos de Amazon FSx formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Regla de AWS Config	Directrices
OPS-07	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Regla de AWS Config	Directrices
OPS-07	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatiz adas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantán ea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
OPS-12	cw-loggroup-retention-period-check	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Regla de AWS Config	Directrices
OPS-12	s3-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).
OPS-13	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de cibersegu ridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Regla de AWS Config	Directrices
OPS-13	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEn abled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
OPS-13	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultado s de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Regla de AWS Config	Directrices
OPS-14	cloud-trail-log-file-validation-enabled	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validació n de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsifica r archivos de registros de CloudTrail sin que se sepa.
OPS-14	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Regla de AWS Config	Directrices
OPS-14	cw-loggroup-retention-period-check	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.
OPS-14	s3-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).
OPS-15	api-gw-execution-logging-enabled	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Regla de AWS Config	Directrices
OPS-15	cloud-trail-cloud-watch-logs-enabled	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su Cuenta de AWS.
OPS-15	codebuild-project-logging-enabled	Asegúrese de que el registro de proyectos de AWS CodeBuild esté habilitado para que los registros de salida de compilación se envíen a Amazon CloudWatch o Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Regla de AWS Config	Directrices
OPS-15	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y que se transmitan a los registros de Amazon CloudWatch para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
OPS-15	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Regla de AWS Config	Directrices
OPS-15	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en los dominios de Amazon OpenSearch Service. Los registros de auditoría le permiten realizar un seguimiento de la actividad en sus dominios de OpenSearch, incluidas las autenticaciones correctas y fallidas, las solicitudes a OpenSearch, los cambios de índice y las consultas de búsqueda entrantes.
OPS-15	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y que se transmitan a los registros de Amazon CloudWatch para su retención y respuesta. Los registros de errores de OpenSearch Service pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Regla de AWS Config	Directrices
OPS-15	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
OPS-15	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Regla de AWS Config	Directrices
OPS-15	s3-bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
OPS-15	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Regla de AWS Config	Directrices
OPS-15	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.
OPS-15	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las Cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Regla de AWS Config	Directrices
OPS-15	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la Cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.
OPS-15	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las prácticas de seguridad recomendadas de AWS para AWS CloudTrail, ya que comprueba la habilitación de varios ajustes, como el uso del cifrado de registros, la validación de registros y la activación de AWS CloudTrail en varias regiones.

ID de control	Regla de AWS Config	Directrices
OPS-15	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones de la Consola de administración de AWS y las llamadas a la API. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP desde donde han realizado las llamadas y en qué momento se han realizado . CloudTrail entregará los archivos de registro de todas las regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Regla de AWS Config	Directrices
OPS-22	ecr-private-image-scanning-enabled	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.
PSS-05	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Regla de AWS Config	Directrices
PSS-05	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
PSS-05	root-account-hardware-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.

ID de control	Regla de AWS Config	Directrices
PSS-05	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.

ID de control	Regla de AWS Config	Directrices
PSS-07	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de

ID de control	Regla de AWS Config	Directrices
		seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñ as de IAM. Los valores reales deben reflejar las políticas de su organización.

Plantilla

La plantilla está disponible en GitHub: Catálogo de criterios de cumplimiento de computación en la nube de Alemania (C5).

Prácticas recomendadas operativas para la Ley Gramm Leach Bliley (GLBA)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre las reglas Gramm-Leach-Bliley Act (GLBA) y AWS Managed Config. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles GLBA. Un control de la GLBA puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la	dms-replication-not-public	Gestione el acceso a la AWS nube

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas		asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiada s para las instituci ones financieras sujetas a su jurisdicc ión en relación con las medidas de protecció n administrativas, técnicas y físicas	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiada s para las instituci ones financieras sujetas a su jurisdicc ión en relación con las medidas de protecció n administrativas, técnicas y físicas	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube aseguránd ose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	autoscaling-launch-config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	api-gw-cache-enabledy cifrado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	codebuild-project-sCifrado con 3 registros	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para AWS CodeBuild los registros almacenados en Amazon S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(1)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (1) para garantizar la seguridad y confidencialidad de los registros y la información de los clientes;	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(2)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (2) para protegerse ante las amenazas o peligros previstos para la seguridad o integridad de dichos registros; y	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(2)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (2) para protegerse ante las amenazas o peligros previstos para la seguridad o integridad de dichos registros; y	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	mfa-enabled-for-iam-acceso desde la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearch Permite un control de acceso al dominio basado en funciones, así como una seguridad a nivel de índices, documentos y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	efs-access-point-enforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
GLBA-SEC.501(b)(3)	De conformidad con la política de la subsección (a), cada agencia o autoridad descrita en la sección 505(a) establecerá las normas apropiadas para las instituciones financieras sujetas a su jurisdicción en relación con las medidas de protección administrativas, técnicas y físicas (3) para protegerse ante el acceso no autorizado a o el uso de dichos registros o información, que podría generar perjuicios o inconveniencias sustanciales a cualquier cliente.	efs-access-point-enforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para la Ley Gramm Leach Bliley (GLBA).

Prácticas operativas recomendadas para el anexo 11 de la UE de GxP

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes

de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el anexo 11 de GxP EU y las reglas de Config AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles del anexo 11 de GxP EU. Un control del anexo 11 de la UE de GxP puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1. Gestión de riesgos	La gestión de riesgos debe aplicarse durante todo el ciclo de vida del sistema informati zado, teniendo en cuenta la seguridad del paciente, la integridad de los datos y la calidad del producto. Como parte de un sistema de gestión de riesgos, las decisiones sobre el alcance de los controles de validació n e integridad de los datos deben basarse en una evaluación del riesgo justifica da y documentada del sistema informati zado.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1. Gestión de riesgos	La gestión de riesgos debe aplicarse durante todo el ciclo de vida del sistema informati zado, teniendo en cuenta la seguridad del paciente, la integridad de los datos y la calidad del producto. Como parte de un sistema de gestión de riesgos, las decisiones sobre el alcance de los controles de validació n e integridad de los datos deben basarse en una evaluación del riesgo justifica da y documentada del sistema informati zado.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2. Validación: control de cambios en la documentación	La documentación de validación debe incluir los registros de control de cambios (si corresponde) e informes sobre cualquier desviación observada durante el proceso de validación.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.3. Validación: inventario	Debería estar disponible una lista actualizada de todos los sistemas relevantes y su funcionalidad de GMP (inventario). En el caso de los sistemas críticos, debe estar disponible una descripción actualizada del sistema en la que se detallen las disposiciones físicas y lógicas, los flujos de datos y las interfaces con otros sistemas o procesos, los requisitos previos de hardware y software y las medidas de seguridad.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Utilice AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.3. Validación: inventario	Debería estar disponible una lista actualizada de todos los sistemas relevantes y su funcionalidad de GMP (inventario). En el caso de los sistemas críticos, debe estar disponible una descripción actualizada del sistema en la que se detallen las disposiciones físicas y lógicas, los flujos de datos y las interfaces con otros sistemas o procesos, los requisitos previos de hardware y software y las medidas de seguridad.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.3. Validación: inventario	Debería estar disponible una lista actualizada de todos los sistemas relevantes y su funcionalidad de GMP (inventario). En el caso de los sistemas críticos, debe estar disponible una descripción actualizada del sistema en la que se detallen las disposiciones físicas y lógicas, los flujos de datos y las interfaces con otros sistemas o procesos, los requisitos previos de hardware y software y las medidas de seguridad.	ec2- -eni-periodic security-group-attached-to	Para ayudarle a administrar su inventario de activos, esta regla comprueba si los grupos de seguridad están vinculados a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a una interfaz de red elástica. Si sus grupos de seguridad no están conectados a estos tipos de recursos, es posible que no se utilicen y que ya no sean necesarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.3. Validación: inventario	Debería estar disponible una lista actualizada de todos los sistemas relevante s y su funcionalidad de GMP (inventar io). En el caso de los sistemas críticos, debe estar disponibl e una descripci ón actualizada del sistema en la que se detallen las disposici ones físicas y lógicas, los flujos de datos y las interfaces con otros sistemas o procesos, los requisito s previos de hardware y software y las medidas de seguridad .	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.3. Validación: inventario	Debería estar disponible una lista actualizada de todos los sistemas relevantes y su funcionalidad de GMP (inventario). En el caso de los sistemas críticos, debe estar disponible una descripción actualizada del sistema en la que se detallen las disposiciones físicas y lógicas, los flujos de datos y las interfaces con otros sistemas o procesos, los requisitos previos de hardware y software y las medidas de seguridad.	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.3. Validación: inventario	Debería estar disponible una lista actualizada de todos los sistemas relevantes y su funcionalidad de GMP (inventario). En el caso de los sistemas críticos, debe estar disponible una descripción actualizada del sistema en la que se detallen las disposiciones físicas y lógicas, los flujos de datos y las interfaces con otros sistemas o procesos, los requisitos previos de hardware y software y las medidas de seguridad.	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validació n debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validació n debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validació n debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validació n debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validació n debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validació n debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validació n debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validación debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validació n debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.8. Validación: transferencia de datos	Si los datos se transfieren a otro formato o sistema de datos, la validació n debe incluir comprobaciones de que el valor o el significado de los datos no se alteren durante este proceso de migración.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Datos	Los sistemas computarizados que intercambian datos electrónicamente con otros sistemas deben incluir las comprobaciones integradas adecuadas para la entrada y el procesamiento correctos y seguros de los datos, a fin de minimizar los riesgos.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1. Almacenamiento de datos: protección contra daños	Los datos deben protegerse por medios físicos y electrónicos contra cualquier daño. Se debe comprobar la accesibilidad, legibilidad y precisión de los datos almacenados. El acceso a los datos debe garantizarse durante todo el período de retención.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	aurora-resources-p rotected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	backup-plan-min-fr equency-and-min-re tention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) y requiredF requencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevantes. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validación y supervisarse periódicamente.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevantes. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validación y supervisarse periódicamente.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperac ión de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establece r el parámetro requiredRetentionD ays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	dynamodb-pitr-enab led	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantiza r que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevantes. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validación y supervisarse periódicamente.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	ebs-resources-prot ected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	efs-resources-prot ected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	fsx-resources-prot ected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2. Almacenamiento de datos: copias de seguridad	Se deben realizar copias de seguridad periódicas de todos los datos relevante s. La integridad y precisión de los datos de respaldo y la capacidad de restaurarlos deben comprobarse durante la validació n y supervisarse periódicamente.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Registros de auditoría	Sobre la base de una evaluación de riesgos, debería considerarse la posibilidad de integrar en el sistema la creación de un registro de todos los cambios y eliminaciones pertinentes a GMP (un “registro de auditoría” generado por el sistema). Para cambiar o eliminar datos relevantes para GMP, se debe documentar el motivo. Los registros de auditoría deben estar disponibles y convertirse en un formato generalmente inteligible y revisarse periódicamente.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Administración de cambios y configura ciones	Cualquier cambio en un sistema informati zado, incluidas las configuraciones del sistema, solo debe realizarse de forma controlada de acuerdo con un procedimiento definido.	elb-deletion-prote ction-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protecció n contra borrado. Utilice esta caracterí stica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibi lidad de sus aplicacio nes.
10. Administración de cambios y configura ciones	Cualquier cambio en un sistema informati zado, incluidas las configuraciones del sistema, solo debe realizarse de forma controlada de acuerdo con un procedimiento definido.	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Administración de cambios y configura ciones	Cualquier cambio en un sistema informati zado, incluidas las configuraciones del sistema, solo debe realizarse de forma controlada de acuerdo con un procedimiento definido.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Evaluación periódica	Los sistemas informatizados deben evaluarse periódica mente para confirmar que permanecen en un estado válido y cumplen con GMP. Dichas evaluacio nes deben incluir, cuando proceda, la gama actual de funciones, los registros de desviacio nes, los incidente s, los problemas, el historial de actualiza ciones y los informes sobre el rendimien to, la fiabilidad, la seguridad y el estado de la validación.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabilitada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	efs-access-point-enforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	efs-access-point-enforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearch Permite un control de acceso al dominio basado en funciones, así como una seguridad a nivel de índices, documentos y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	rds-instance-iam-authentication-habilitado	Asegúrese de que la autenticación AWS Identity and Access Management (IAM) esté habilitada en las instancias del Amazon Relational Database Service (Amazon RDS) para controlar el acceso a los sistemas y activos. De esta manera se fuerza el cifrado del tráfico de red hacia y desde la base de datos mediante la capa de sockets seguros (SSL). No es necesario almacenar credenciales de usuario en la base de datos, ya que la autenticación se administra de forma externa.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomienda utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.1. Seguridad: personas autorizadas	Deben and/or existir controles físicos y lógicos para restringir el acceso al sistema computarizado a las personas autorizadas. Los métodos adecuados para impedir la entrada no autorizada al sistema pueden incluir el uso de llaves, tarjetas de acceso, códigos personales con contraseña, datos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenamiento de datos.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.3. Seguridad: registro de auditoría de autorizaciones	La creación, el cambio y la cancelación de las autorizaciones de acceso deben registrarse.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican , confirman o eliminan datos, incluidas la fecha y la hora.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican , confirman o eliminan datos, incluidas la fecha y la hora.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican, confirman o eliminan datos, incluidas la fecha y la hora.	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican, confirman o eliminan datos, incluidas la fecha y la hora.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican, confirman o eliminan datos, incluidas la fecha y la hora.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican, confirman o eliminan datos, incluidas la fecha y la hora.	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican, confirman o eliminan datos, incluidas la fecha y la hora.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican, confirman o eliminan datos, incluidas la fecha y la hora.	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican , confirman o eliminan datos, incluidas la fecha y la hora.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican , confirman o eliminan datos, incluidas la fecha y la hora.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican, confirman o eliminan datos, incluidas la fecha y la hora.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.4. Seguridad: registro de auditoría	Los sistemas de gestión de datos y documentos deben diseñarse para registrar la identidad de los operadores que introducen, modifican , confirman o eliminan datos, incluidas la fecha y la hora.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13. Administración de incidentes	Todos los incidentes, no solo los fallos del sistema y los errores de datos, deben notificarse y evaluarse. Se debe identificar la causa raíz de un incidente crítico y debe constituir la base de las acciones correctivas y preventivas.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13. Administración de incidentes	Todos los incidentes, no solo los fallos del sistema y los errores de datos, deben notificarse y evaluarse . Se debe identific ar la causa raíz de un incidente crítico y debe constituir la base de las acciones correctivas y preventiv as.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	aurora-resources-p rotected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	backup-plan-min-fr equency-and-min-re tention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) y requiredF requencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	ebs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	efs-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantiza r una alta disponibi lidad, asegúrese de que su ELB tenga instancias registrad as de varias zonas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	elb-cross-zone-loa d-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	lambda-vpc-multi-az-comprobar	Si su función AWS Lambda está configurada para conectarse a una nube privada virtual (VPC) de su cuenta, implemente la función AWS Lambda en al menos dos zonas de disponibilidad diferentes para asegurarse de que su función esté disponibl e para procesar eventos en caso de una interrupción del servicio en una sola zona.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	opensearch-data-node-fault-tolerancia	Amazon OpenSearch Service (OpenSearch Servicio) requiere al menos tres nodos de datos para una alta disponibilidad y tolerancia a errores. La implementación de un dominio OpenSearch de servicio con al menos tres nodos de datos garantiza las operaciones del clúster en caso de que un nodo falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informatizados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuidad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternativos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamente documentadas y comprobadas.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	rds-cluster-multi-az-habilitado	Los clústeres de Amazon Relationa l Database Service (Amazon RDS) deben tener habilitada la replicación Multi-AZ para facilitar la disponibilidad de los datos almacenad os. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
16. Continuidad empresarial	Para garantizar la disponibilidad de sistemas informati zados que respalden los procesos críticos, deben tomarse medidas para garantizar la continuid ad del soporte de dichos procesos en caso de avería del sistema (por ejemplo, un sistema manual o alternativo). El tiempo necesario para poner en práctica los mecanismos alternati vos debe basarse en el riesgo y ser adecuado para un sistema concreto y el proceso empresarial que respalde. Estas disposiciones deben estar debidamen te documentadas y comprobadas.	vpc-vpn-2-tunnels-up	Se pueden implement ar túneles Site-to-S ite VPN redundant es para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectivi dad en caso de que una de las conexione s Site-to-Site VPN no esté disponibl e. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	aurora-resources-p rotected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	backup-plan-min-fr equency-and-min-re tention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) y requiredF requencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	backup-recovery-po int-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	backup-recovery-po int-manual-elimina ción-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperac ión. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	backup-recovery-po int-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperac ión de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establece r el parámetro requiredRetentionD ays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	dynamodb-pitr-enab led	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantiza r que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	ebs-optimized-inst ance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operation s. This optimization provides the most efficient performan ce for your EBS volumes by minimizin g contention between Amazon EBS I/O EBS y otro tráfico de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	ebs-resources-prot ected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	efs-resources-prot ected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	fsx-resources-prot ected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
17. Archivado	Los datos pueden archivarse. Se debe comprobar la accesibilidad, legibilidad e integrida d de estos datos. Si se van a hacer cambios relevante s en el sistema (por ejemplo, en equipos o programas informáticos), se debe garantiza r y comprobar la capacidad de recuperación de los datos.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

Plantilla

La plantilla está disponible en el GitHub anexo 11 de las mejores prácticas operativas para la GxP de la UE.

Prácticas operativas recomendadas para la seguridad de la HIPAA

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el

cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) y las reglas de AWS Config gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de la HIPAA. Un control de la HIPAA puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este paquete de conformidad ha sido validado por AWS Security Assurance Services LLC (AWS SAS), que está formado por un equipo de asesores de seguridad cualificados en el sector de las tarjetas de pago (QSAs), profesionales certificados por HITRUST en el marco de seguridad común (CCSFPs) y profesionales del cumplimiento certificados para ofrecer orientación y evaluaciones en relación con diversos marcos industriales. AWS Los profesionales de SAS diseñaron este paquete de conformidad para permitir a los clientes ajustarse a un subconjunto de la HIPAA.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(A)	(A) Análisis de riesgos (obligatorio). Realice una evaluación precisa y exhaustiva de los posibles riesgos y vulnerabilidades en relación con la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida en poder de la entidad cubierta.	annual-risk-assessment-performed (Verificación del proceso)	Realice una evaluación anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determinar la probabilidad y el impacto de los riesgos y and/or vulnerabilidades identificados que afectan a una organización.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).		de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrai l entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	dms-replication-not-public	Gestiona el acceso a la AWS nube asegurándote de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	efs-encrypted-check	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	rds-snapshot-encry pted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	sagemaker-notebook -instance-kms-conf igurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligato rio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(1)(ii)(B)	(B) Gestión de riesgos (obligatorio). Implemente las medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiado a fin de cumplir con la Sección 164.306(a).	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimi entos para garantiza r que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a) (4) de esta sección obtengan acceso a la información médica electrónica protegida.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,308(a)(3)(i)	(3)(i) Norma: seguridad de la fuerza laboral. Implemente políticas y procedimientos para garantizar que todos los miembros de su fuerza laboral tengan un acceso adecuado a la información médica electrónica protegida, según lo dispuesto en el párrafo (a)(4) de esta sección, y para evitar que los miembros de la fuerza laboral que no tengan acceso en virtud del párrafo (a)(4) de esta sección obtengan acceso a la información médica electrónica protegida.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	cloud-trail-cloud-watch-Habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(A)	(A) and/or Supervisión de autorizaciones (direccionable). Implemente procedimientos para la and/or supervisión de las autorizaciones de los miembros de la fuerza laboral que trabajan con información de salud electrónica protegida o en lugares donde se pueda acceder a ella.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimi entos para determina r si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(B)	(B) Procedimiento de autorización de la fuerza laboral (direccionable). Implemente procedimientos para determinar si el acceso de un miembro de la fuerza laboral a la información médica electrónica protegida es apropiado.	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(3)(ii)(C)	(C) Procedimientos de rescisión (direccionable). Implemente procedimientos para rescindir el acceso a la información médica electrónica protegida cuando finalice la relación contractual de un miembro de la fuerza laboral o según lo exijan las determinaciones tomadas en virtud de lo especificado en el párrafo (a)(3)(ii)(B) de esta sección.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consistentes con los requisitos aplicables de la subparte E de la presente parte.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consisten tes con los requisito s aplicables de la subparte E de la presente parte.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consistentes con los requisitos aplicables de la subparte E de la presente parte.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consistentes con los requisitos aplicables de la subparte E de la presente parte.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consistentes con los requisitos aplicables de la subparte E de la presente parte.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consistentes con los requisitos aplicables de la subparte E de la presente parte.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consisten tes con los requisito s aplicables de la subparte E de la presente parte.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consistentes con los requisitos aplicables de la subparte E de la presente parte.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consistentes con los requisitos aplicables de la subparte E de la presente parte.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(i)	(4)(i) Norma: gestión del acceso a la información. Implemente políticas y procedimientos para autorizar el acceso a la información médica electrónica protegida que sean consisten tes con los requisito s aplicables de la subparte E de la presente parte.	s3- bucket-acl-prohibi ted	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercamb io de información sobre la atención médica forma parte de una organizac ión más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la informaci ón médica electrónica protegida del centro de intercambio de información contra el acceso no autorizad o por parte de la organización más grande.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomienda utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(A)	(A) Aislamiento de las funciones del centro de intercambio de información sobre la atención médica (obligatorio). Si un centro de intercambio de información sobre la atención médica forma parte de una organización más grande, el centro de intercambio de información debe implementar políticas y procedimientos que protejan la información médica electrónica protegida del centro de intercambio de información contra el acceso no autorizado por parte de la organización más grande.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccio nable). Implemente políticas y procedimi entos para otorgar acceso a la informaci ón médica electróni ca protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacci ón, programa, proceso u otro mecanismo.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccio nable). Implemente políticas y procedimi entos para otorgar acceso a la informaci ón médica electróni ca protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacci ón, programa, proceso u otro mecanismo.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(B)	(B) Autorización de acceso (direccionable). Implemente políticas y procedimientos para otorgar acceso a la información médica electrónica protegida, por ejemplo, mediante el acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomienda utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccio nable). Implemente políticas y procedimi entos que, en función de las políticas de autorización de acceso de la entidad, establezc an, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomienda utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(4)(ii)(C)	(C) Establecimiento y modificación del acceso (direccionable). Implemente políticas y procedimientos que, en función de las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso del usuario a una estación de trabajo, transacción, programa o proceso.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(A)	(A) Recordatorios de seguridad (direccionable). Actualizaciones de seguridad periódicas.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(A)	(A) Recordatorios de seguridad (direccionable). Actualizaciones de seguridad periódicas.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(A)	(A) Recordatorios de seguridad (direccionable). Actualizaciones de seguridad periódicas.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(A)	(A) Recordatorios de seguridad (direccionable). Actualizaciones de seguridad periódicas.	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(B)	(B) Protección contra software malicioso (direccionable). Procedimientos para protegerse del software malintencionado, detectarlo y denunciarlo.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(B)	(B) Protección contra software malicioso (direccionable). Procedimientos para protegerse del software malintencionado, detectarlo y denunciarlo.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(B)	(B) Protección contra software malicioso (direccionable). Procedimientos para protegerse del software malintencionado, detectarlo y denunciarlo.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(C)	(C) Supervisión del inicio de sesión (direccionable). Procedimientos para supervisar los intentos de inicio de sesión y reportar discrepan cias.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(C)	(C) Supervisión del inicio de sesión (direccionable). Procedimientos para supervisar los intentos de inicio de sesión y reportar discrepan cias.	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a las API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(C)	(C) Supervisión del inicio de sesión (direccionable). Procedimientos para supervisar los intentos de inicio de sesión y reportar discrepan cias.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(5)(ii)(D)	(D) Gestión de contraseñas (direccionable). Procedimientos para crear, cambiar y proteger las contraseñas.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(6)(i)	(6)(i) Norma: procedimientos para incidentes de seguridad. Implemente políticas y procedimientos para abordar los incidentes de seguridad.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(6)(ii)	(ii) Especificación de implementación: respuesta e informes (obligatorio). Identifiq ue y responda a los incidentes de seguridad sospechos os o conocidos; mitigue, en la medida de lo posible, los efectos perjudiciales de los incidentes de seguridad de los que tenga conocimie nto la entidad cubierta; y documente los incidentes de seguridad y sus resultados.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimi entos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(i)	(7)(i) Norma: plan de contingencia. Establezca (e implemente, según sea necesario) políticas y procedimientos para responder a una emergencia u otro suceso (por ejemplo, un incendio, un vandalismo, una falla del sistema y un desastre natural) que dañe los sistemas que contienen información de salud electrónica protegida.	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligatorio). Establezca e implemente procedimientos para crear y mantener copias exactas recuperables de la información de salud electrónica protegida.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligato rio). Establezca e implemente procedimi entos para crear y mantener copias exactas recuperab les de la información de salud electrónica protegida.	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(A)	(A) Plan de respaldo de datos (obligatorio). Establezca e implemente procedimientos para crear y mantener copias exactas recuperables de la información de salud electrónica protegida.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que establezcas el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(B)	(B) Plan de recuperación ante desastres (obligatorio). Establezca (e implemente según sea necesario) procedimientos para restaurar cualquier pérdida de datos.	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(C)	(C) Plan de operación en modo de emergencia (obligatorio). Establezca (e implemente según sea necesario) procedimientos que permitan continuar con los procesos empresariales críticos para proteger la seguridad de la información médica electrónica protegida mientras se opera en modo de emergencia.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(C)	(C) Plan de operación en modo de emergencia (obligatorio). Establezca (e implemente según sea necesario) procedimientos que permitan continuar con los procesos empresariales críticos para proteger la seguridad de la información médica electrónica protegida mientras se opera en modo de emergencia.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(C)	(C) Plan de operación en modo de emergencia (obligatorio). Establezca (e implemente según sea necesario) procedimientos que permitan continuar con los procesos empresariales críticos para proteger la seguridad de la información médica electrónica protegida mientras se opera en modo de emergencia.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(C)	(C) Plan de operación en modo de emergencia (obligatorio). Establezca (e implemente según sea necesario) procedimientos que permitan continuar con los procesos empresariales críticos para proteger la seguridad de la información médica electrónica protegida mientras se opera en modo de emergencia.	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(C)	(C) Plan de operación en modo de emergencia (obligatorio). Establezca (e implemente según sea necesario) procedimientos que permitan continuar con los procesos empresariales críticos para proteger la seguridad de la información médica electrónica protegida mientras se opera en modo de emergencia.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(7)(ii)(C)	(C) Plan de operación en modo de emergencia (obligatorio). Establezca (e implemente según sea necesario) procedimientos que permitan continuar con los procesos empresariales críticos para proteger la seguridad de la información médica electrónica protegida mientras se opera en modo de emergencia.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(8)	(8) Norma: evaluación. Realice una evaluación periódica técnica y no técnica, basada inicialmente en las normas implementadas en virtud de esta regla y, posteriormente, en respuesta a los cambios ambientales u operativos que afecten a la seguridad de la información médica protegida por medios electrónicos, para establecer en qué medida las políticas y procedimientos de seguridad de una entidad cumplen con los requisitos de esta subparte.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.308(a)(8)	(8) Norma: evaluación. Realice una evaluación periódica técnica y no técnica, basada inicialmente en las normas implementadas en virtud de esta regla y, posteriormente, en respuesta a los cambios ambientales u operativos que afecten a la seguridad de la información médica protegida por medios electrónicos, para establecer en qué medida las políticas y procedimientos de seguridad de una entidad cumplen con los requisitos de esta subparte.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiendan utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en 164.308(a)(4).	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(1)	(a)(1) Norma: control de acceso. Implemente políticas y procedimientos técnicos para los sistemas de información electrónica que mantienen la información médica electrónica protegida a fin de permitir el acceso únicamente a aquellas personas o programas de software a los que se les hayan otorgado los derechos de acceso, tal como se especifica en ¤ 164.308(a)(4).	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(i)	(2) Especificaciones de implementación: (i) Identificación de usuario única (obligatorio). Asigne un and/or número de nombre único para identificar y rastrear la identidad del usuario.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligato rio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligato rio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligato rio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(ii)	(ii) Procedimiento de acceso de emergencia (obligatorio). Establezca (e implemente según sea necesario) los procedimientos para obtener la información de salud electrónica protegida necesaria durante una emergencia.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros. AWS CloudTrail

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccio nable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(a)(2)(iv)	(iv) Cifrado y descifrado (direccionable). Implemente un mecanismo para cifrar y descifrar la información de salud electrónica protegida.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a las API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad de los sistemas de información que contienen o utilizan información de salud electrónica protegida.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad de los sistemas de información que contienen o utilizan información de salud electrónica protegida.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimi entos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad de los sistemas de información que contienen o utilizan información de salud electrónica protegida.	s3- event-notifications-enabled	Las notificaciones de eventos de Amazon S3 pueden alertar al personal pertinente de cualquier modificación accidental o intencionada en los objetos de su bucket. Algunos ejemplos de alertas son: creación de un objeto nuevo, eliminación de objetos, restauración de objetos, objetos perdidos o replicados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(b)	(b) Norma: controles de auditoría . Implemente mecanismos de hardware, software y and/or procedimientos que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,312(c)(1)	(c)(1) Norma: integridad. Implemente políticas y procedimientos para proteger la información de salud electrónica protegida contra la alteración o destrucción indebidas.	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,312(c)(1)	(c)(1) Norma: integridad. Implemente políticas y procedimientos para proteger la información de salud electrónica protegida contra la alteración o destrucción indebidas.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,312(c)(1)	(c)(1) Norma: integridad. Implemente políticas y procedimientos para proteger la información de salud electrónica protegida contra la alteración o destrucción indebidas.	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164,312(c)(1)	(c)(1) Norma: integridad. Implemente políticas y procedimientos para proteger la información de salud electrónica protegida contra la alteración o destrucción indebidas.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
164,312(c)(1)	(c)(1) Norma: integridad. Implemente políticas y procedimientos para proteger la información de salud electrónica protegida contra la alteración o destrucción indebidas.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(c)(2)	(2) Especificación de implementación: mecanismo para autenticar la información de salud electrónica protegida (direccionable). Implemente mecanismos electrónicos para corroborar que la información de salud electrónica protegida no haya sido alterada o destruida de manera no autorizada.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(c)(2)	(2) Especificación de implementación: mecanismo para autenticar la información de salud electrónica protegida (direccionable). Implemente mecanismos electrónicos para corroborar que la información de salud electrónica protegida no haya sido alterada o destruida de manera no autorizada.	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
164.312(c)(2)	(2) Especificación de implementación: mecanismo para autenticar la información de salud electrónica protegida (direccionable). Implemente mecanismos electrónicos para corroborar que la información de salud electrónica protegida no haya sido alterada o destruida de manera no autorizada.	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(c)(2)	(2) Especificación de implementación: mecanismo para autenticar la información de salud electrónica protegida (direccionable). Implemente mecanismos electrónicos para corroborar que la información de salud electrónica protegida no haya sido alterada o destruida de manera no autorizada.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(c)(2)	(2) Especificación de implementación: mecanismo para autenticar la información de salud electrónica protegida (direccionable). Implemente mecanismos electrónicos para corroborar que la información de salud electrónica protegida no haya sido alterada o destruida de manera no autorizada.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(d)	(d) Norma: autenticación de personas o entidades. Implemente procedimientos para verificar que la persona o entidad que busca acceder a información médica electrónica protegida sea la persona reclamada.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(d)	(d) Norma: autenticación de personas o entidades. Implemente procedimientos para verificar que la persona o entidad que busca acceder a información médica electrónica protegida sea la persona reclamada.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(d)	(d) Norma: autenticación de personas o entidades. Implemente procedimientos para verificar que la persona o entidad que busca acceder a información médica electrónica protegida sea la persona reclamada.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(d)	(d) Norma: autenticación de personas o entidades. Implemente procedimientos para verificar que la persona o entidad que busca acceder a información médica electrónica protegida sea la persona reclamada.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(d)	(d) Norma: autenticación de personas o entidades. Implemente procedimientos para verificar que la persona o entidad que busca acceder a información médica electrónica protegida sea la persona reclamada.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo dentro de Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	account-level-public-accesss3- -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibi lidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(1)	(e)(1) Norma: seguridad de transmisión. Implemente medidas técnicas de seguridad para evitar el acceso no autorizado a la información de salud electrónica protegida que se transmita a través de una red de comunicaciones electrónicas.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(e)(2)(i)	(i) Controles de integridad (direccionable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmitida electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(i)	(i) Controles de integridad (direccio nable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmiti da electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
164.312(e)(2)(i)	(i) Controles de integridad (direccio nable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmiti da electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(i)	(i) Controles de integridad (direccio nable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmiti da electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(i)	(i) Controles de integridad (direccionable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmitida electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
164.312(e)(2)(i)	(i) Controles de integridad (direccionable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmitida electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(i)	(i) Controles de integridad (direccionable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmitida electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(e)(2)(i)	(i) Controles de integridad (direccionable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmitida electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(i)	(i) Controles de integridad (direccionable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmitida electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
164.312(e)(2)(i)	(i) Controles de integridad (direccionable). Implemente medidas de seguridad para garantizar que la información de salud electrónica protegida transmitida electrónicamente no se modifique indebidamente sin ser detectada hasta que se elimine.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros. AWS CloudTrail
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.312(e)(2)(ii)	(ii) Cifrado (direccionable). Implemente un mecanismo para cifrar la información de salud electrónica protegida cuando lo considere pertinente.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(1)	(b)(1) Norma: requisitos para los planes de salud grupales. Salvo cuando la única información médica electrónica protegida divulgada al patrocinador del plan se divulgue de conformidad con el ¤ 164.504(f)(1)(ii) o (iii), o según lo autorizado en el ¤ 164.508, un plan de salud grupal debe asegurarse de que los documentos de su plan indiquen que el patrocinador del plan protegerá de manera razonable y adecuada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al patrocinador del plan de salud grupal o por él en nombre del plan de salud grupal.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón médica electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurars e de que la separació n adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldad a por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrai l registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón médica electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurars e de que la separació n adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldad a por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón médica electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurars e de que la separació n adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldad a por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón médica electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurars e de que la separació n adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldad a por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón médica electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurars e de que la separació n adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldad a por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón médica electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurars e de que la separació n adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldad a por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón médica electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurars e de que la separació n adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldad a por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón médica electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurars e de que la separació n adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldad a por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal; (ii) Asegurarse de que la separación adecuada requerida por el ¤ 164.504(f)(2) (iii) esté respaldada por medidas de seguridad adecuadas y razonables; (iii) Garantizar que cualquier agente,	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	incluido un subcontratista, al que proporcione esta información, se comprometa a implementar medidas de seguridad razonables y apropiadas para proteger la información; y (iv) Notificar al plan de salud grupal cualquier incidente de seguridad del que tenga conocimiento.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad. Esta regla requiere que establezca una política de seguridad predefinida para sus oyentes de SSL. La

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	elb-cross-zone-load-habilitado para el balanceo	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposici ones que exijan al patrocinador del plan: (i) Implementar medidas de protecció n administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibi lidad de la informaci ón de salud electróni ca protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo dentro de Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
164.314(b)(2)(i)	(2) Especificaciones de implementación (obligatorio). Los documentos del plan de salud grupal deben modificarse para incorporar disposiciones que exijan al patrocinador del plan: (i) Implementar medidas de protección administrativas, físicas y técnicas que protejan de manera razonable y adecuada la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida que cree, reciba, mantenga o transmita en nombre del plan de salud grupal;	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para la seguridad según la HIPAA.

Prácticas operativas recomendadas para IRS 1075

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear comprobaciones de control de seguridad, operativas o de optimización de

costos mediante reglas de AWS Config administradas o personalizadas y acciones correctivas de AWS Config. Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de asignación entre la IRS 1075 y las reglas de AWS Config administradas. Cada regla de Config se aplica a un recurso de AWS específico que está relacionado con uno o más controles de la IRS 1075. Un control de la IRS 1075 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube d. Cifrado de datos en tránsito	El FTI debe estar cifrado en tránsito dentro del entorno de la nube. Todos los mecanismos utilizados para cifrar el FTI deben contar con la certificación FIPS 140 y funcionar con los últimos módulos compatibl es con la FIPS 140. Este requisito debe incluirse en el SLA.	alb-http-to-https-redirection-check	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.3.1 Computación en la nube d. Cifrado de datos en tránsito	El FTI debe estar cifrado en tránsito dentro del entorno de la nube. Todos los mecanismos utilizados para cifrar el FTI deben contar	elasticsearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticse arch Service esté habilitado. El cifrado de nodo a nodo

ID de control	Descripción del control	Regla de AWS Config	Directrices
	con la certificación FIPS 140 y funcionar con los últimos módulos compatibl es con la FIPS 140. Este requisito debe incluirse en el SLA.		habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
3.3.1 Computación en la nube d. Cifrado de datos en tránsito	El FTI debe estar cifrado en tránsito dentro del entorno de la nube. Todos los mecanismos utilizados para cifrar el FTI deben contar con la certificación FIPS 140 y funcionar con los últimos módulos compatibl es con la FIPS 140. Este requisito debe incluirse en el SLA.	elb-tls-https-listeners-only	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube d. Cifrado de datos en tránsito	El FTI debe estar cifrado en tránsito dentro del entorno de la nube. Todos los mecanismos utilizados para cifrar el FTI deben contar con la certificación FIPS 140 y funcionar con los últimos módulos compatibl es con la FIPS 140. Este requisito debe incluirse en el SLA.	opensearch-https-r equired	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, asegúrese de que HTTPS esté activado para las conexiones en sus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube d. Cifrado de datos en tránsito	El FTI debe estar cifrado en tránsito dentro del entorno de la nube. Todos los mecanismos utilizados para cifrar el FTI deben contar con la certificación FIPS 140 y funcionar con los últimos módulos compatibles con la FIPS 140. Este requisito debe incluirse en el SLA.	opensearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube d. Cifrado de datos en tránsito	El FTI debe estar cifrado en tránsito dentro del entorno de la nube. Todos los mecanismos utilizados para cifrar el FTI deben contar con la certificación FIPS 140 y funcionar con los últimos módulos compatibl es con la FIPS 140. Este requisito debe incluirse en el SLA.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.3.1 Computación en la nube d. Cifrado de datos en tránsito	El FTI debe estar cifrado en tránsito dentro del entorno de la nube. Todos los mecanismos utilizados para cifrar el FTI deben contar con la certificación FIPS 140 y funcionar con los últimos módulos compatibl es con la FIPS 140. Este requisito debe incluirse en el SLA.	s3-bucket-ssl-requ ests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	api-gw-cache-enabled-and-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos de recuperación de AWS Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se cifran con una clave maestra de cliente (CMK) propiedad de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	ec2-ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	elasticsearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service (OpenSearch Service).
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	opensearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service.
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	s3-bucket-server-side-encryption-enabled	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	s3-default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	sagemaker-endpoint-configuration-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenciales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	sagemaker-notebook-instance-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenciales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube e. Cifrado de datos en reposo	Cifrado de datos en reposo: el FTI debe cifrarse mientras esté en reposo en la nube mediante el último mecanismo de cifrado certificado por la FIPS 140. Este requisito debe incluirse en el SLA.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para los secretos de AWS Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube k. Autenticación multifactor	Las agencias deben implementar una autenticación multifactorial suficiente cuando sus soluciones en la nube estén disponibles en Internet (es decir, cuando se pueda acceder a la solución en la nube desde fuera de la red de confianza de la agencia).	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube k. Autenticación multifactor	Las agencias deben implementar una autenticación multifactorial suficiente cuando sus soluciones en la nube estén disponibles en Internet (es decir, cuando se pueda acceder a la solución en la nube desde fuera de la red de confianza de la agencia).	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube k. Autenticación multifactor	Las agencias deben implementar una autenticación multifactorial suficiente cuando sus soluciones en la nube estén disponibles en Internet (es decir, cuando se pueda acceder a la solución en la nube desde fuera de la red de confianza de la agencia).	root-account-hardware-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.1 Computación en la nube k. Autenticación multifactor	Las agencias deben implementar una autenticación multifactorial suficiente cuando sus soluciones en la nube estén disponibles en Internet (es decir, cuando se pueda acceder a la solución en la nube desde fuera de la red de confianza de la agencia).	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las Cuentas de AWS comprometidas.
3.3.1 Computación en la nube i. Evaluación de riesgos:	La agencia debe realizar una evaluación anual de los controles de seguridad y privacidad establecidos en todos los sistemas de información utilizados para recibir, procesar, almacenar, acceder, proteger o transmitir el FTI.	annual-risk-assessment-performed (verificación del proceso)	Realice una evaluación anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determinar la probabilidad y el impacto de los riesgos o vulnerabilidades identificados que afecten a una organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	guardduty-non-archived-findings	Amazon GuardDuty le ayuda a comprender el efecto de un incidente al clasificar los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional daysLowSev (valor predeterminado de Config: 30), daysMediumSev (valor predeterminado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	netfw-policy-rule-group-associated	Una política de AWS Network Firewall define la forma en que su firewall monitorea y gestiona el tráfico en una Amazon VPC. Puede configurar grupos de reglas sin y con estado para filtrar los paquetes y los flujos de tráfico, y definir la administración del tráfico predeterminado.
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	netfw-stateless-rule-group-not-empty	Un grupo de reglas de AWS Network Firewall contiene reglas que definen cómo el firewall procesa el tráfico en la VPC. Un grupo de reglas sin estado vacío, cuando está presente en una política de firewall, no procesa el tráfico.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	waf-regional-rule-not-empty	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencadenar un comportamiento no deseado.
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	waf-regional-rulegroup-not-empty	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportamiento no deseado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	waf-regional-webacl-not-empty	Una ACL web asociada a un AWS WAF puede contener una colección de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicaciones web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3.3.6 Límites e infraestructura de red	Las agencias deben implementar dispositivos de protección de límites en toda la arquitectura de sus sistemas, incluidos routers, firewalls, conmutadores y sistemas de detección de intrusos para proteger los FTI y los sistemas de los FTI.	api-gw-associated-with-waf	AWS WAF permite configurar un conjunto de reglas (denominadas lista de control de acceso web (ACL web) que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (f)	Cree, habilite, modifique, deshabilite y elimine cuentas de acuerdo con los requisitos previos de los procedimientos de administración de cuentas de la agencia;	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (f)	Cree, habilite, modifique, deshabilite y elimine cuentas de acuerdo con los requisitos previos de los procedimientos de administración de cuentas de la agencia;	account-part-of-organizations	La administración centralizada de Cuentas de AWS dentro de AWS Organizations contribuye a garantizar la conformidad de las cuentas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (f)	Cree, habilite, modifique, deshabilite y elimine cuentas de acuerdo con los requisitos previos de los procedimientos de administración de cuentas de la agencia;	iam-root-access-key-check	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de Cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (f)	Cree, habilite, modifique, deshabilite y elimine cuentas de acuerdo con los requisitos previos de los procedimientos de administración de cuentas de la agencia;	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (f)	Cree, habilite, modifique, deshabilite y elimine cuentas de acuerdo con los requisitos previos de los procedimientos de administración de cuentas de la agencia;	iam-user-no-policies-check	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (g)	Supervise el uso de las cuentas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las Cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (g)	Supervise el uso de las cuentas	cloud-trail-cloud-watch-logs-enabled	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su Cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (g)	Supervise el uso de las cuentas	cloud-trail-log-file-validation-enabled	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (g)	Supervise el uso de las cuentas	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (g)	Supervise el uso de las cuentas	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (g)	Supervise el uso de las cuentas	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (g)	Supervise el uso de las cuentas	s3-bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (g)	Supervise el uso de las cuentas	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	secretsmanager-scheduled-rotation-success-check	Esta regla garantiza que los secretos de AWS Secrets Manager se distribuyan correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	secretsmanager-secret-periodic-rotation	Esta regla garantiza que los secretos de AWS Secrets Manager tengan habilitada la rotación periódica. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencial mente, reducir el impacto sobre la empresa si el secreto se desvela. El valor predeterminado es 90 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	secretsmanager-secret-unused	Si existen credenciales no utilizadas en AWS Secrets Manager, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedForDays (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireLowercaseCh aracters (valor de Prácticas recomenda das de seguridad básica de AWS: true), RequireSy mbols (valor de Prácticas recomenda das de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	iam-root-access-key-check	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de Cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	iam-user-no-policies-check	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-2 Administración de cuentas (j)	Revise las cuentas para comprobar que cumplen con los requisitos de administración de cuentas	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
(CE-1) Sistema automatizado de administración de cuentas	Facilite la administración de cuentas del sistema mediante mecanismos automatizados.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
(CE-1) Sistema automatizado de administración de cuentas	Facilite la administración de cuentas del sistema mediante mecanismos automatizados.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
(CE-1) Sistema automatizado de administración de cuentas	Facilite la administración de cuentas del sistema mediante mecanismos automatizados.	secretsmanager-scheduled-rotation-success-check	Esta regla garantiza que los secretos de AWS Secrets Manager se distribuyan correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	Regla de AWS Config	Directrices
(CE-3): Desactivación de cuentas	Desactive las cuentas en un plazo de 120 días cuando las cuentas: a. Hayan caducado; b. Ya no estén asociadas a un usuario o individuo ; c. Estén infringiendo la política de la organización; o d. Lleven 120 días inactivas para las cuentas sin privilegios y 60 días para las cuentas con privilegios	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
(CE-12) Supervisión de cuentas para detectar un uso atípico	Supervise las cuentas del sistema para detectar el uso atípico definido por la agencia; y notifique el uso atípico de las cuentas del sistema al personal o las funciones definidas por la agencia.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, lo que impide que las políticas incluyan acciones bloqueadas en todas las claves del AWS Key Management Service. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el parámetro blockedActionsPatterns. (Valor de las prácticas recomendadas de seguridad básica de AWS: kms:Decrypt, kms:ReEncryptFrom). Los valores reales deben reflejar las

ID de control	Descripción del control	Regla de AWS Config	Directrices
			políticas de su organización.
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	opensearch-access-control-enabled	Asegúrese de habilitar el control de acceso detallado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con privilegio mínimo a los dominios de Amazon OpenSearch Service. Permite el control de acceso al dominio basado en roles, así como la seguridad en el nivel de índices, documentos y campos, la compatibilidad con los paneles de OpenSearch Service, la tenencia múltiple y la autenticación básica HTTP para OpenSearch Service y Kibana.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	secretsmanager-secret-unused	Si existen credenciales no utilizadas en AWS Secrets Manager, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedForDays (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	codebuild-project-environment-privileged-check	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de que su entorno de proyecto de Amazon CodeBuild no tenga habilitado el modo con privilegios. Esta configuración debe estar deshabilitada para evitar el acceso no deseado a las API de Docker, así como al hardware subyacente del contenedor.
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	ec2-instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	ecs-task-definition-nonroot-user	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	efs-access-point-enforce-user-identity	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en el Amazon Elastic File System (Amazon EFS). Cuando está habilitada, Amazon EFS reemplaza los ID de usuario y grupo del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario obligatoria.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	Regla de AWS Config	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC-6 Privilegio mínimo	Utilice el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas.	iam-user-no-policies-check	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
			básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisito s de configura ción y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	root-account-hardware-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	api-gw-execution-logging-enabled	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	cloud-trail-cloud-watch-logs-enabled	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su Cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y que se transmitan a los registros de Amazon CloudWatch para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisito s de configura ción y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administr ación de AWS y las llamadas a la API. Puede identificar los usuarios y las Cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y que se transmitan a los registros de Amazon CloudWatch para su retención y respuesta. Los registros de errores de OpenSearch Service pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisito s de configura ción y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisito s de configura ción y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisito s de configura ción y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	s3-bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisito s de configura ción y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisitos de configuración y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AC-17: Acceso remoto	Establezca y documente las restricciones de uso, los requisito s de configura ción y conexión y las directrices de implementación para cada tipo de acceso remoto permitido; y autorice cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.	redshift-enhanced-vpc-routing-enabled	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AT-1: Concienciación y formación	Imparta formación sobre conocimientos básicos sobre seguridad y privacidad a los usuarios del sistema (incluidos gerentes, altos ejecutivos y contratistas)	security-awareness-program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
AU-2: Eventos de auditoría	Identifique los tipos de eventos que el sistema es capaz de registrar para facilitar la función de auditoría	audit-log-policy-exists (verificación del proceso)	Establezca y mantenga una política de administración de registros de auditoría que defina los requisitos de registro de su organización. Esto incluye, pero no se limita a, la revisión y la conservación de los registros de auditoría.

ID de control	Descripción del control	Regla de AWS Config	Directrices
AU-16: Registro de auditorías interorganizacionales	Utilice métodos definidos por la agencia para coordinar la información de auditoría definida por la agencia entre las organizaciones externas cuando la información de auditoría se transmita a través de los límites de la organización.	audit-log-policy-exists (verificación del proceso)	Establezca y mantenga una política de administración de registros de auditoría que defina los requisitos de registro de su organización. Esto incluye, pero no se limita a, la revisión y la conservación de los registros de auditoría.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CA-7: Monitoreo continuo	Desarrollo de una estrategia de monitoreo continuo en el nivel de sistema e implementación de un monitoreo continuo de acuerdo con la estrategia de monitoreo continuo en el nivel de la organización: establecimiento de métricas definidas por la agencia que deban monitorearse; evaluaciones de control continuas de acuerdo con la estrategia de monitoreo continuo; monitoreo continuo de las métricas definidas por el sistema y la organización de acuerdo con la estrategia de monitoreo continuo; correlación y análisis de la información generada por las evaluaciones del control y la supervisión; acciones de	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	respuesta para abordar los resultados del análisis del control información de evaluación y monitoreo; y notificación del estado de seguridad y privacidad del sistema al personal definido por la agencia anualmente, como mínimo.		

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	aurora-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de copia de seguridad de datos, asegúrese de que su plan de AWS Backup esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer los parámetros requiredFrequencyValue (valor predeterminado de Config: 1), requiredRetentionDays (valor predeterminado de Config: 35) y

ID de control	Descripción del control	Regla de AWS Config	Directrices
			requiredFrequencyUnit (valor predeterminado de Config: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos de recuperación de AWS Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	backup-recovery-point-manual-deletion-disabled	Asegúrese de que los puntos de recuperación de AWS Backup tengan adjunta una política basada en los recursos que impida eliminar los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	backup-recovery-point-minimum-retention-check	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus puntos de recuperación de AWS Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (valor predeterminado de Config: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalme nte; c. Realización de copias de seguridad de la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidenc ialidad, integridad y disponibilidad de la información de copias de seguridad.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalme nte; c. Realización de copias de seguridad de la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidenc ialidad, integridad y disponibilidad de la información de copias de seguridad.	dynamodb-in-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus tablas de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalme nte; c. Realización de copias de seguridad de la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidenc ialidad, integridad y disponibilidad de la información de copias de seguridad.	ebs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	ec2-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalme nte; c. Realización de copias de seguridad de la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidenc ialidad, integridad y disponibilidad de la información de copias de seguridad.	efs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administr ado con una solución de copia de seguridad basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	elasticache-redis-cluster-automatic-backup-check	Cuando se habilitan las copias de seguridad automáticas, Amazon ElastiCache crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	fsx-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus sistemas de archivos de Amazon FSx formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	rds-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un plan de AWSBackup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documentación del sistema, incluida la documentación relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalmente; c. Realización de copias de seguridad de la documentación del sistema, incluida la documentación relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidencialidad, integridad y disponibilidad de la información de copias de seguridad.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
CP-9: Copias de seguridad del sistema	a. Realización de copias de seguridad semanales de la información en el nivel de usuario contenida en la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad; b. Realización de copias de seguridad de la información en el nivel del sistema contenida en el sistema semanalme nte; c. Realización de copias de seguridad de la documenta ción del sistema, incluida la documenta ción relacionada con la seguridad y la privacidad, semanalmente; y d. Proteja la confidenc ialidad, integridad y disponibilidad de la información de copias de seguridad.	s3-bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-2: Identificación y autenticación (usuarios de la organización) (CE-1) Autenticación multifactor en cuentas con privilegios	Implementación de la autenticación multifactorial para acceder a cuentas con privilegios	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-2: Identificación y autenticación (usuarios de la organización) (CE-1) Autenticación multifactor en cuentas con privilegios	Implementación de la autenticación multifactorial para acceder a cuentas con privilegios	root-account-hardware-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las Cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-2: Identificación y autenticación (usuarios de la organización) (CE-2) Autenticación multifactor en cuentas sin privilegios	Implementación de la autenticación multifactorial para acceder a cuentas sin privilegios	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
IA-5: Administración del autenticador: (CE-1) Autenticación basada en contraseñas: para la autenticación basada en contraseñas	Imponga las siguientes reglas de composición y complejidad: 1. Imponga una longitud mínima de contraseña de catorce (14) caracteres. 2. Imponga una complejidad mínima de contraseña para que contenga una combinación de números, letras mayúsculas, minúsculas y caracteres especiales. 3. Exija al menos un (1) cambio de carácter cuando se seleccionen nuevas contraseñas para su uso. 4. Almacene y transmita únicamente contraseñas protegidas criptográficamente. 5. Imponga restricciones de duración de las contraseñas: i. Un (1) día como mínimo y 90 días como máximo. ii. Las contraseñas de las cuentas de servicio	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad

ID de control	Descripción del control	Regla de AWS Config	Directrices
	caducarán en un plazo de 366 días (incluidos).		básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
PM-5: Inventario del sistema	Desarrolle y actualice continuamente un inventario de los sistemas de la organización.	ec2-instance-managed-by-systems-manager	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
PM-5: Inventario del sistema	Desarrolle y actualice continuamente un inventario de los sistemas de la organización.	ec2-managedinstance-association-compliance-status-check	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
PM-5: Inventario del sistema	Desarrolle y actualice continuamente un inventario de los sistemas de la organización.	vpc-network-acl-unused-check	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.
PM-5: Inventario del sistema	Desarrolle y actualice continuamente un inventario de los sistemas de la organización.	ec2-volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
RA-5: Monitoreo y escaneo de vulnerabilidades	Supervise y analice las vulnerabilidades en el sistema y las aplicaciones alojadas cada treinta (30) días, antes de instalar un nuevo sistema de información en la red de la agencia, para confirmar las medidas correctivas y cuando se identifiquen y notifiquen nuevas vulnerabilidades que puedan afectar al sistema	vuln-scans-performed (verificación del proceso)	Asegúrese de que los escaneos de vulnerabilidades se realicen de acuerdo con sus requisitos de cumplimiento. Su organización debe definir la cadencia del escaneo, las herramientas utilizadas y el uso de los resultados.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-10: Administración de la configuración para desarrolladores (e.)	Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-10: Administración de la configuración para desarrolladores (e.)	Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].	guardduty-non-archived-findings	Amazon GuardDuty le ayuda a comprender el efecto de un incidente al clasificar los resultados por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional daysLowSev (valor predeterminado de Config: 30), daysMediumSev (valor predeterminado de Config: 7) y daysHighSev (valor predeterminado de Config: 1) para los resultados no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-10: Administración de la configuración para desarrolladores (e.)	Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SA-10: Administración de la configuración para desarrolladores (a) (c.)	Administre la configuración durante el diseño, el desarrollo, la implementación y la operación del sistema, componente o servicio; implemente únicamente los cambios aprobados por la organización en el sistema, componente o servicio;	ec2-instance-managed-by-systems-manager	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-4: Información sobre los recursos del sistema compartidos	Evitar la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema	ec2-volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de informaci ón únicamente a través de interface s administradas que consistan en dispositi vos de protección de límites dispuesto s de acuerdo con una arquitectura de seguridad de la organización.	rds-instance-public-access-check	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de informaci ón únicamente a través de interface s administradas que consistan en dispositi vos de protección de límites dispuesto s de acuerdo con una arquitectura de seguridad de la organización.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de informaci ón únicamente a través de interface s administradas que consistan en dispositi vos de protección de límites dispuesto s de acuerdo con una arquitectura de seguridad de la organización.	redshift-cluster-public-access-check	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de información únicamente a través de interfaces administradas que consistan en dispositivos de protección de límites dispuestos de acuerdo con una arquitectura de seguridad de la organización.	ebs-snapshot-public-restorable-check	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de información únicamente a través de interfaces administradas que consistan en dispositivos de protección de límites dispuestos de acuerdo con una arquitectura de seguridad de la organización.	ec2-instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de información únicamente a través de interfaces administradas que consistan en dispositivos de protección de límites dispuestos de acuerdo con una arquitectura de seguridad de la organización.	lambda-function-public-access-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de informaci ón únicamente a través de interface s administradas que consistan en dispositi vos de protección de límites dispuesto s de acuerdo con una arquitectura de seguridad de la organización.	s3-account-level-p ublic-access-blocks-periodic	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterm inado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben

ID de control	Descripción del control	Regla de AWS Config	Directrices
			reflejar las políticas de su organización.
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de información únicamente a través de interfaces administradas que consistan en dispositivos de protección de límites dispuestos de acuerdo con una arquitectura de seguridad de la organización.	s3-bucket-policy-grantee-check	Gestione el acceso a la nube de AWS habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso concedido por el bucket de Amazon S3 esté restringido por cualquiera de las entidades principales de AWS, usuarios federados, entidades principales de servicio, direcciones IP o ID de Amazon Virtual Private Cloud (Amazon VPC) que proporcione.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de informaci ón únicamente a través de interface s administradas que consistan en dispositi vos de protección de límites dispuesto s de acuerdo con una arquitectura de seguridad de la organización.	s3-bucket-public-read-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizad os acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de información únicamente a través de interfaces administradas que consistan en dispositivos de protección de límites dispuestos de acuerdo con una arquitectura de seguridad de la organización.	s3-bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de informaci ón únicamente a través de interface s administradas que consistan en dispositi vos de protección de límites dispuesto s de acuerdo con una arquitectura de seguridad de la organización.	sagemaker-notebook -no-direct-internet-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites	Supervise y controle las comunicaciones en el límite externo del sistema y en los límites internos clave del sistema; implemente subredes para los componentes del sistema de acceso público que estén separados de las redes organizativas internas; y Conéctese a redes externas o sistemas de informaci ón únicamente a través de interface s administradas que consistan en dispositi vos de protección de límites dispuesto s de acuerdo con una arquitectura de seguridad de la organización.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: La protección de límites (CE-9) restringe el tráfico amenazante de comunicaciones salientes	Detecte y deniegue el tráfico de comunicaciones salientes que suponga una amenaza para los sistemas externos y audite la identidad de los usuarios internos relacionados con las comunicaciones denegadas.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: La protección de límites (CE-9) restringe el tráfico amenazante de comunicaciones salientes	Detecte y deniegue el tráfico de comunicaciones salientes que suponga una amenaza para los sistemas externos y audite la identidad de los usuarios internos relacionados con las comunicaciones denegadas.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicaciones web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: La protección de límites (CE-9) restringe el tráfico amenazante de comunicaciones salientes	Detecte y deniegue el tráfico de comunicaciones salientes que suponga una amenaza para los sistemas externos y audite la identidad de los usuarios internos relacionados con las comunicaciones denegadas.	api-gw-associated-with-waf	AWS WAF permite configurar un conjunto de reglas (denominadas lista de control de acceso web (ACL web) que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-7: Protección de límites (definida por el IRS)	Las agencias deberán implement ar y gestionar la protección de límites (normalmente mediante firewalls) en los límites de confianza. Se debe monitorear cada límite de confianza y se deben controlar las comunicaciones a través de cada límite.	netfw-policy-rule-group-associated	Una política de AWS Network Firewall define la forma en que su firewall monitorea y gestiona el tráfico en una Amazon VPC. Puede configurar grupos de reglas sin y con estado para filtrar los paquetes y los flujos de tráfico, y definir la administr ación del tráfico predeterminado.
SC-7: Protección de límites (definida por el IRS)	Las agencias deberán implement ar y gestionar la protección de límites (normalmente mediante firewalls) en los límites de confianza. Se debe monitorear cada límite de confianza y se deben controlar las comunicaciones a través de cada límite.	netfw-stateless-rule-group-not-empty	Un grupo de reglas de AWS Network Firewall contiene reglas que definen cómo el firewall procesa el tráfico en la VPC. Un grupo de reglas sin estado vacío, cuando está presente en una política de firewall, no procesa el tráfico.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8: Protección criptográfica de confidencialidad e integridad de la transmisión (CE-1)	Implemente mecanismos criptográficos para evitar la divulgación no autorizada de información y detectar cambios en la información durante la transmisión.	alb-http-to-https-redirection-check	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8: Protección criptográfica de confidencialidad e integridad de la transmisión (CE-1)	Implemente mecanismos criptográficos para evitar la divulgación no autorizada de información y detectar cambios en la información durante la transmisión.	elasticsearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8: Protección criptográfica de confidencialidad e integridad de la transmisión (CE-1)	Implemente mecanismos criptográficos para evitar la divulgación no autorizada de información y detectar cambios en la información durante la transmisión.	elb-tls-https-listeners-only	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8: Protección criptográfica de confidencialidad e integridad de la transmisión (CE-1)	Implemente mecanismos criptográficos para evitar la divulgación no autorizada de información y detectar cambios en la información durante la transmisión.	opensearch-https-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, asegúrese de que HTTPS esté activado para las conexiones en sus dominios de Amazon OpenSearch Service.
SC-8: Protección criptográfica de confidencialidad e integridad de la transmisión (CE-1)	Implemente mecanismos criptográficos para evitar la divulgación no autorizada de información y detectar cambios en la información durante la transmisión.	opensearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-8: Protecció n criptográfica de confidencialidad e integridad de la transmisión (CE-1)	Implemente mecanismos criptográ ficos para evitar la divulgación no autorizada de información y detectar cambios en la información durante la transmisión.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8: Protecció n criptográfica de confidencialidad e integridad de la transmisión (CE-1)	Implemente mecanismos criptográ ficos para evitar la divulgación no autorizada de información y detectar cambios en la información durante la transmisión.	s3-bucket-ssl-requ ests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-12: Establecimiento y administración de claves criptográficas	La agencia debe establecer y administrar las claves criptográficas cuando se emplee la criptografía en el sistema de acuerdo con los siguientes requisitos de administración de claves: NIST SP 800-57, recomendación para la administración de claves, para la generación, distribución, almacenamiento, acceso y destrucción de claves.	kms-cmk-not-scheduled-for-deletion	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMK) necesarias no estén programadas para borrado en AWS Key Management Service (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-12: Establecimiento y administración de claves criptográficas	La agencia debe establecer y administrar las claves criptográficas cuando se emplee la criptografía en el sistema de acuerdo con los siguientes requisitos de administración de claves: NIST SP 800-57, recomendación para la administración de claves, para la generación, distribución, almacenamiento, acceso y destrucción de claves.	cmk-backing-key-rotation-enabled	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar certificados SSL/TLS públicos y privados con servicios de AWS y recursos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	alb-http-to-https-redirection-check	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	api-gw-cache-enabled-and-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	elasticsearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	elb-tls-https-listeners-only	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	opensearch-https-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, asegúrese de que HTTPS esté activado para las conexiones en sus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	opensearch-node-to-node-encryption-check	Asegúrese de que el cifrado de nodo a nodo para Amazon Elasticsearch Service esté habilitado. El cifrado de nodo a nodo habilita el cifrado TLS 1.2 para todas las comunicaciones dentro de la Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos de recuperación de AWS Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se cifran con una clave maestra de cliente (CMK) propiedad de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	ec2-ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	opensearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	s3-default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para los secretos de AWS Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	elasticsearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service (OpenSearch Service).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	s3-bucket-server-side-encryption-enabled	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	s3-bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	sagemaker-endpoint-configuration-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenciales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	sagemaker-notebook-instance-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenciales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-13: Protección criptográfica	Implemente los siguientes tipos de criptografía necesarios para cada uso criptográfico especificado: el mecanismo de cifrado más reciente validado por FIPS-140, NIST 800-52, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), cifrado en tránsito (cifrado de carga útil) Se prohíbe el uso del SHA-1 para las firmas digitales.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-23: Autenticidad de las sesiones	Proteja la autenticidad de las sesiones de comunicación.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El método IMDSv2 utiliza controles basados en sesiones. IMDSv2 permite implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	api-gw-cache-enabled-and-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos de recuperación de AWS Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se cifran con una clave maestra de cliente (CMK) propiedad de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	ec2-ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	elasticsearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service (OpenSearch Service).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	opensearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (valor predeterminado de Config: TRUE) y loggingEnabled (valor predeterminado de Config: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	s3-bucket-server-side-encryption-enabled	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	s3-default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	sagemaker-endpoint-configuration-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenciales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	sagemaker-notebook-instance-kms-key-configured	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenciales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SC-28: Protección de la información en reposo (CE-1) Protección criptográfica	Implementación de mecanismos criptográficos para evitar la divulgación y modificación no autorizadas del FTI en reposo en los sistemas informáticos de los usuarios finales (es decir, computadoras de sobremesa, computadoras portátiles, dispositivos móviles y dispositivos de almacenamiento portátiles y extraíbles) en un almacenamiento no volátil.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para los secretos de AWS Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2: Corrección de defectos (definida por el IRS)	La agencia se asegurará de que, al encenderse y conectarse diariamente a la red de la agencia, las estaciones de trabajo (tal y como se definen en la política, incluidas las conexiones remotas mediante estaciones de trabajo GFE) se comprueben para asegurarse de que se hayan aplicado los parches más recientes aprobados por la agencia y de que cualquier parche nuevo o ausente se aplique según sea necesario o se revise de otro modo, al menos, cada 24 horas (excepto fines de semana, festivos, etc.).	ec2-instance-managed-by-systems-manager	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2: Corrección de defectos (definida por el IRS)	La agencia se asegurará de que, al encenderse y conectarse diariamente a la red de la agencia, las estaciones de trabajo (tal y como se definen en la política, incluidas las conexiones remotas mediante estaciones de trabajo GFE) se comprueben para asegurarse de que se hayan aplicado los parches más recientes aprobados por la agencia y de que cualquier parche nuevo o ausente se aplique según sea necesario o se revise de otro modo, al menos, cada 24 horas (excepto fines de semana, festivos, etc.).	ec2-managedinstance-association-compliance-status-check	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2: Corrección de defectos (definida por el IRS)	La agencia se asegurará de que, al encenderse y conectarse diariamente a la red de la agencia, las estaciones de trabajo (tal y como se definen en la política, incluidas las conexiones remotas mediante estaciones de trabajo GFE) se comprueben para asegurarse de que se hayan aplicado los parches más recientes aprobados por la agencia y de que cualquier parche nuevo o ausente se aplique según sea necesario o se revise de otro modo, al menos, cada 24 horas (excepto fines de semana, festivos, etc.).	ec2-managedinstance-patch-compliance-status-check	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2: Corrección de defectos (definida por el IRS)	La agencia se asegurará de que, al encenderse y conectarse diariamente a la red de la agencia, las estaciones de trabajo (tal y como se definen en la política, incluidas las conexiones remotas mediante estaciones de trabajo GFE) se comprueben para asegurarse de que se hayan aplicado los parches más recientes aprobados por la agencia y de que cualquier parche nuevo o ausente se aplique según sea necesario o se revise de otro modo, al menos, cada 24 horas (excepto fines de semana, festivos, etc.).	ecs-fargate-latest-platform-version	Las actualizaciones y los parches de seguridad se implementan automáticamente para las tareas de AWS Fargate. Si se encuentra un problema de seguridad que afecta a una versión de la plataforma de AWS Fargate, AWS parchea la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de los servicios para utilizar la versión de plataforma más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2: Corrección de defectos (definida por el IRS)	La agencia se asegurará de que, al encenderse y conectarse diariamente a la red de la agencia, las estaciones de trabajo (tal y como se definen en la política, incluidas las conexiones remotas mediante estaciones de trabajo GFE) se comprueben para asegurarse de que se hayan aplicado los parches más recientes aprobados por la agencia y de que cualquier parche nuevo o ausente se aplique según sea necesario o se revise de otro modo, al menos, cada 24 horas (excepto fines de semana, festivos, etc.).	elastic-beanstalk-managed-updates-enabled	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-2: Corrección de defectos (definida por el IRS)	La agencia se asegurará de que, al encenderse y conectarse diariamente a la red de la agencia, las estaciones de trabajo (tal y como se definen en la política, incluidas las conexiones remotas mediante estaciones de trabajo GFE) se comprueben para asegurarse de que se hayan aplicado los parches más recientes aprobados por la agencia y de que cualquier parche nuevo o ausente se aplique según sea necesario o se revise de otro modo, al menos, cada 24 horas (excepto fines de semana, festivos, etc.).	rds-automatic-minor-version-upgrade-enabled	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema	La organización: a. Monitorea el sistema de informaci ón para detectar: 1. Los ataques y los indicadores de posibles ataques de acuerdo con [Misión: objetivos de monitoreo definidos por la organización]; y 2. Las conexione s locales, de red y remotas no autorizad as; b. Identifica el uso no autorizado del sistema de informaci ón mediante [Asignaci ón: técnicas y métodos definidos por la organización]; c. Implementa dispositi vos de monitoreo: 1. Estratégicamente dentro del sistema de información para recopilar información esencial determina da por la organizac ión; y 2. En ubicacion es específicas del sistema para rastrear tipos específicos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización; d. Protege la informaci ón obtenida mediante las herramientas de monitoreo de intrusion es contra el acceso, la modificación y la eliminación no autorizados;		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema	La organización: a. Monitorea el sistema de información para detectar: 1. Los ataques y los indicadores de posibles ataques de acuerdo con [Misión: objetivos de monitoreo definidos por la organización]; y 2. Las conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [Asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: 1. Estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y 2. En ubicaciones específicas del sistema para rastrear tipos específicos	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización; d. Protege la informaci ón obtenida mediante las herramientas de monitoreo de intrusion es contra el acceso, la modificación y la eliminación no autorizados;		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema	La organización: a. Monitorea el sistema de información para detectar: 1. Los ataques y los indicadores de posibles ataques de acuerdo con [Misión: objetivos de monitoreo definidos por la organización]; y 2. Las conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [Asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: 1. Estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y 2. En ubicaciones específicas del sistema para rastrear tipos específicos	cloudwatch-alarm-action-check	Las alarmas de Amazon CloudWatch avisan cuando una métrica supera el umbral durante un número específico de periodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (valor predeterminado de Config: True), insufficientDataActionRequired (valor predeterminado de Config: True) y okActionRequired (valor predeterminado de Config: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización; d. Protege la informaci ón obtenida mediante las herramientas de monitoreo de intrusion es contra el acceso, la modificación y la eliminación no autorizados;		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema	La organización: a. Monitorea el sistema de informaci ón para detectar: 1. Los ataques y los indicadores de posibles ataques de acuerdo con [Misión: objetivos de monitoreo definidos por la organización]; y 2. Las conexione s locales, de red y remotas no autorizad as; b. Identifica el uso no autorizado del sistema de informaci ón mediante [Asignaci ón: técnicas y métodos definidos por la organización]; c. Implementa dispositi vos de monitoreo: 1. Estratégicamente dentro del sistema de información para recopilar información esencial determina da por la organizac ión; y 2. En ubicacion es específicas del sistema para rastrear tipos específicos	cloud-trail-cloud-watch-logs-enabled	Utilice Amazon CloudWatch para recopilar y administr ar de forma centraliz ada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su Cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización; d. Protege la informaci ón obtenida mediante las herramientas de monitoreo de intrusion es contra el acceso, la modificación y la eliminación no autorizados;		

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema	La organización: a. Monitorea el sistema de informaci ón para detectar: 1. Los ataques y los indicadores de posibles ataques de acuerdo con [Misión: objetivos de monitoreo definidos por la organización]; y 2. Las conexione s locales, de red y remotas no autorizad as; b. Identifica el uso no autorizado del sistema de informaci ón mediante [Asignaci ón: técnicas y métodos definidos por la organización]; c. Implementa dispositi vos de monitoreo: 1. Estratégicamente dentro del sistema de información para recopilar información esencial determina da por la organizac ión; y 2. En ubicacion es específicas del sistema para rastrear tipos específicos	ec2-instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
	de transacciones de interés para la organización; d. Protege la informaci ón obtenida mediante las herramientas de monitoreo de intrusion es contra el acceso, la modificación y la eliminación no autorizados;		
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilar án y conservarán, durante al menos un año, la información de los encabezad os del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en los dominios de Amazon OpenSearch Service. Los registros de auditoría le permiten realizar un seguimiento de la actividad en sus dominios de OpenSearch, incluidas las autenticaciones correctas y fallidas, las solicitudes a OpenSearch, los cambios de índice y las consultas de búsqueda entrantes.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	s3-bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	api-gw-execution-logging-enabled	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	cloud-trail-cloud-watch-logs-enabled	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su Cuenta de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las Cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	cloud-trail-log-file-validation-enabled	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-4: Monitoreo del sistema (definido por el IRS)	Todos los puntos o portales de acceso a Internet recopilarán y conservarán, durante al menos un año, la información de los encabezados del tráfico entrante y saliente, con exclusión de las conexiones “anónimas” de Internet aprobadas, según lo autorice el CISO de la agencia.	cw-loggroup-retention-period-check	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-7: Integridad del software, el firmware y la información	Utilice herramientas de verificación de integridad para detectar cambios no autorizados en el siguiente software, firmware e información: núcleos del sistema, controladores, firmware (por ejemplo, BIOS, UEFI), software (por ejemplo, sistema operativo, aplicaciones, middleware) y atributos de seguridad.	ec2-instance-managed-by-systems-manager	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-7: Integridad del software, el firmware y la información	Utilice herramientas de verificación de integridad para detectar cambios no autorizados en el siguiente software, firmware e información: núcleos del sistema, controladores, firmware (por ejemplo, BIOS, UEFI), software (por ejemplo, sistema operativo, aplicaciones, middleware) y atributos de seguridad.	ec2-managedinstance-patch-compliance-status-check	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-7: Integridad del software, el firmware y la información	Utilice herramientas de verificación de integridad para detectar cambios no autorizados en el siguiente software, firmware e información: núcleos del sistema, controladores, firmware (por ejemplo, BIOS, UEFI), software (por ejemplo, sistema operativo, aplicaciones, middleware) y atributos de seguridad.	cloud-trail-log-file-validation-enabled	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	dynamodb-in-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus tablas de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	dynamodb-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	ebs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	ebs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	ec2-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	efs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administr ado con una solución de copia de seguridad basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	efs-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	elasticache-redis-cluster-automatic-backup-check	Cuando se habilitan las copias de seguridad automátic as, Amazon ElastiCac he crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	fsx-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus sistemas de archivos de Amazon FSx formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	rds-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus recursos de Amazon Relational Database Service (Amazon RDS) formen parte de un plan de AWSBackup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	aurora-resources-protected-by-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de copia de seguridad de datos, asegúrese de que su plan de AWS Backup esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer los parámetros requiredFrequencyValue (valor predeterminado de Config: 1), requiredRetentionDays (valor predeterminado de Config: 35) y

ID de control	Descripción del control	Regla de AWS Config	Directrices
			requiredFrequencyUnit (valor predeterminado de Config: days). El valor real debe reflejar los requisitos de su organización.
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	backup-recovery-point-manual-deletion-disabled	Asegúrese de que los puntos de recuperación de AWS Backup tengan adjunta una política basada en los recursos que impida eliminar los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	backup-recovery-point-minimum-retention-check	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus puntos de recuperación de AWS Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (valor predeterminado de Config: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	s3-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	s3-version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transició n de objetos a otra clase de almacenam iento, su archivado o su eliminación tras transcurrir un periodo de tiempo especific ado).

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la información producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas, directrices y requisitos operativos aplicables.	s3-bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	Regla de AWS Config	Directrices
SI-12: Administración y retención de la información	Administre y retenga la información del sistema y la informaci ón producida por el sistema de conformid ad con las leyes, órdenes ejecutivas, directivas, reglament os, políticas, normas, directrices y requisitos operativos aplicables.	s3-bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

Plantilla

La plantilla está disponible en GitHub: Operational Best Practices for IRS 1075.

Prácticas operativas recomendadas para K-ISMS

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre Corea: Sistema de gestión de seguridad de la información (ISMS) y reglas de Config AWS administradas. Cada regla de Config se aplica a un recurso de AWS específico que está relacionado con uno o más controles de Korea - ISMS. Un control de Korea - ISMS puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	AWS Regla de configuración	Directrices
1.2.1	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.
1.2.1	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminaci ón al finalizar una instancia . Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.
2.1.3	ec2- -comprobar managedin stance-association-complian ce-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software

ID de control	AWS Regla de configuración	Directrices
		dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.
2.1.3	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminaci ón al finalizar una instancia . Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
2.3.3	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
2.3.3	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
2.5.1	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
2.5.1	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
2.5.1	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
2.5.1	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
2.5.1	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
2.5.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
2.5.1	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
2.5.1	iam-root-access-key-comprue be	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorpora r el principio de funcionalidad mínima.
2.5.1	iam-user-mfa-enabled	Active esta regla para restringi r el acceso a los recursos en la AWS nube. Esta regla garantiza que la autentica ción multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidente s de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
2.5.1	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
2.5.1	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
2.5.1	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
2.5.1	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
2.5.1	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
2.5.3	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
2.5.3	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
2.5.3	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
2.5.4	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
2.5.5	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
2.5.5	iam-root-access-key-comprob ar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorpora r el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
2.5.5	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS
2.6	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
2.6	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
2.6	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
2.6	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
2.6	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
2.6	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
2.6	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
2.6	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
2.6	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
2.6	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
2.6	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
2.6	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
2.6	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
2.6	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
2.6	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
2.6	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
2.6	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
2.6	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
2.6	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
2.6	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
2.6.6	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
2.6.6	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
2.6.6	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.
2.6.6	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
2.6.6	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
2.6.6	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
2.6.6	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
2.6.6	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
2.6.6	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
2.6.6	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
2.6.6	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
2.6.6	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
2.6.7	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
2.7	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.
2.7	alb-http-drop-invalid-encab ezado activado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
2.7	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
2.7	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
2.7	cloudwatch-log-group-encryp ted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
2.7	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.

ID de control	AWS Regla de configuración	Directrices
2.7	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
2.7	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
2.7	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
2.7	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
2.7	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2.7	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
2.7	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2.7	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
2.7	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
2.7	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
2.7	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
2.7	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
2.7	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
2.7	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2.7	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
2.7	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
2.7	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
2.7	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	AWS Regla de configuración	Directrices
2.7	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2.7.1	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	AWS Regla de configuración	Directrices
2.7.1	elb-predefined-security-policy-ssl-check	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes de SSL de su Classic Elastic Load Balancing utilicen una política de seguridad predefinida. Elastic Load Balancing proporciona configuraciones predefinidas de negociación SSL que se utilizan para la negociación SSL cuando se establece una conexión entre un cliente y el equilibrador de carga. Las configuraciones de la negociación SSL proporcio nan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográ ficos de alta seguridad. Esta regla requiere que establezc a una política de seguridad predefinida para sus oyentes de SSL. La política de seguridad predeterminada es: Policy-TLS-1-2-2017-0. ELBSecurity El valor real debe reflejar las políticas de su organización.
2.7.2	cmk-backing-key-rotation-ha bilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	AWS Regla de configuración	Directrices
2.7.2	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
2.8.5	codebuild-project-envvar-aw scred-comprobar	Asegúrese de que las credenciales AWS_ACCES S_KEY_ID de autenticación AWS_SECRET_ACCESS_ KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	AWS Regla de configuración	Directrices
2.8.5	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personale s ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild . AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credencia les de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
2.8.6	codebuild-project-envvar-aw scred-comprobar	Asegúrese de que las credenciales AWS_ACCES S_KEY_ID de autenticación AWS_SECRET_ACCESS_ KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	AWS Regla de configuración	Directrices
2.8.6	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
2.9.1	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
2.9.1	cloudtrail-security-trail-enabled	Esta regla ayuda a garantiza r el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, al comprobar la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
2.9.1	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	AWS Regla de configuración	Directrices
2.9.1	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automatedSnapshotRetentionPeriodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
2.9.2	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	AWS Regla de configuración	Directrices
2.9.2	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	AWS Regla de configuración	Directrices
2.9.2	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentag e de cuenta (Config Default: 80). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
2.9.2	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
2.9.2	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	AWS Regla de configuración	Directrices
2.9.2	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	AWS Regla de configuración	Directrices
2.9.3	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.
2.9.3	dynamodb-autoscaling-enable d	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimien to aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/writ e capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	AWS Regla de configuración	Directrices
2.9.3	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
2.9.3	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
2.9.3	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
2.9.3	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.
2.9.3	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	AWS Regla de configuración	Directrices
2.9.3	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
2.9.3	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
2.9.3	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
2.9.3	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
2.9.3	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
2.9.3	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
2.9.3	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	AWS Regla de configuración	Directrices
2.9.3	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
2.9.3	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
2.9.3	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalment e administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
2.9.4	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
2.9.4	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
2.9.4	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
2.9.4	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
2.9.4	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.
2.9.4	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilad os proporcionan información detallada sobre las solicitud es enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
2.9.4	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
2.9.4	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
2.9.4	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
2.9.4	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
2.9.4	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	AWS Regla de configuración	Directrices
2.10.3	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.
2.10.3	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
2.10.3	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.
2.10.3	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
2.10.3	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
2.10.5	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
2.10.5	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
2.10.5	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2.10.5	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
2.10.5	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
2.10.5	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2.10.5	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2.10.5	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
2.10.8	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.
2.10.8	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
2.11.2	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
2.11.3	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.
2.11.3	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	AWS Regla de configuración	Directrices
2.11.3	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
2.11.3	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	AWS Regla de configuración	Directrices
2.11.3	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	AWS Regla de configuración	Directrices
2.11.3	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
2.12	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	AWS Regla de configuración	Directrices
2.12	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
2.12	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
2.12	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
2.12	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
2.12	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.
2.12	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	AWS Regla de configuración	Directrices
2.12	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
2.12	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
2.12	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
2.12	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
2.12	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
2.12	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
2.12	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
2.12	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	AWS Regla de configuración	Directrices
2.12	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
2.12	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
2.12	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config default: days). El valor real debe reflejar los requisitos de su organización.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el K-ISMS.

Prácticas operativas recomendadas para el equilibrado de carga

Este paquete de conformidad contiene AWS Config reglas basadas en el equilibrio de carga interno AWS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para el equilibrio de carga.

Prácticas operativas recomendadas para el registro

Este paquete de conformidad contiene AWS Config reglas basadas en el inicio de sesión interno AWS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para el registro.

Prácticas operativas recomendadas para servicios de administración y gobernanza

Este paquete de conformidad contiene AWS Config reglas basadas en los servicios de administración y gobierno. Para obtener más información, consulte Administración y gobierno en AWS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para los servicios de gestión y gobierno.

Prácticas operativas recomendadas para MAS Notice 655

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante

reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el Aviso 655 de la Autoridad Monetaria de Singapur (MAS): Cyber Hygiene AWS y las reglas de Config gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles del MAS Notice 655: Cyber Hygiene. Un control de MAS Notice 655 – Cyber Hygiene puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	AWS Regla de configuración	Directrices
4.1	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
4.1	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se

ID de control	AWS Regla de configuración	Directrices
		reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.
4.1	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
4.1	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
4.1	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS
4.1	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	AWS Regla de configuración	Directrices
4.1	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencrip tar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
4.1	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
4.1	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
4.1	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
4.1	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
4.1	iam-user-mfa-enabled	Active esta regla para restringi r el acceso a los recursos de la AWS nube. Esta regla garantiza que la autentica ción multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidente s de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
4.1	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
4.1	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
4.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
4.1	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
4.1	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
4.1	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.
4.1	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
4.1	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
4.2	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
4.2	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
4.2	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
4.2	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que establezca el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
4.2	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.
4.2	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
4.2	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancia s de Amazon Relational Database Service (RDS) para garantizar que estén instalada s las últimas actualizaciones de las versiones secundari as del sistema de administr ación de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.
4.2	ecr-private-image-scanning-habilitado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.

ID de control	AWS Regla de configuración	Directrices
4.3	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
4.3	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
4.3	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
4.3	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
4.4	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
4.4	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
4.4	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
4.4	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
4.4	ec2- -eni-periódico security-group-attached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.
4.4	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
4.4	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
4.4	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de cibersegu ridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
4.4	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
4.4	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
4.4	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
4.4	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
4.4	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configura ción, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamien to lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
4.4	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
4.4	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
4.4	waf-regional-rule-not-vacío	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencadenar un comportamiento no deseado.

ID de control	AWS Regla de configuración	Directrices
4.4	waf-regional-rulegroup-not-vacío	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportamiento no deseado.
4.4	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.
4.4	netfw-policy-default-action-paquetes de fragmentos	Una política AWS de Network Firewall define la forma en que su firewall supervisa y gestiona el tráfico en una Amazon VPC. Puede configurar grupos de reglas sin y con estado para filtrar los paquetes y los flujos de tráfico. Si se establece de forma predeterminada una acción de pase, es posible que se produzca tráfico no deseado.

ID de control	AWS Regla de configuración	Directrices
4.4	netfw-policy-default-action-paquetes completos	Una política AWS de Network Firewall define la forma en que su firewall supervisa y gestiona el tráfico en una Amazon VPC. Puede configurar grupos de reglas sin y con estado para filtrar los paquetes y los flujos de tráfico. Si se establece de forma predeterminada una acción de pase, es posible que se produzca tráfico no deseado.
4.4	netfw-policy-rule-group-asociado	Una política AWS de Network Firewall define la forma en que su firewall supervisa y gestiona el tráfico en una Amazon VPC. Puede configurar grupos de reglas sin y con estado para filtrar los paquetes y los flujos de tráfico, y definir la administración del tráfico predeterminado.
4.4	netfw-stateless-rule-group-no está vacío	Un grupo de reglas de AWS Network Firewall contiene reglas que definen cómo el firewall procesa el tráfico en la VPC. Un grupo de reglas sin estado vacío, cuando está presente en una política de firewall, no procesa el tráfico.

ID de control	AWS Regla de configuración	Directrices
4.4	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
4.4	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
4.4	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
4.4	sagemaker-notebook-no-direc t-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	AWS Regla de configuración	Directrices
4.4	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
4.4	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
4.4	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
4.4	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
4.4	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	AWS Regla de configuración	Directrices
4.4	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
4.4	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
4.4	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
4.4	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	AWS Regla de configuración	Directrices
4.4	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
4.4	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
4.4	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
4.5	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
4.5	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
4.5	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.
4.5	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de cibersegu ridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
4.6	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
4.6	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
4.6	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
4.6	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
4.6	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
4.6	iam-user-mfa-enabled	Active esta regla para restringi r el acceso a los recursos en la AWS nube. Esta regla garantiza que la autentica ción multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidente s de cuentas compromet idas exigiendo la MFA a los usuarios.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el MAS Notice 655.

Prácticas operativas recomendadas para MAS TRMG

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre las Directrices de gestión del riesgo tecnológico (TRMG) de enero de 2021 de la Autoridad Monetaria de Singapur (MAS) y las reglas de Config AWS gestionadas. Cada regla de AWS Config se aplica a un AWS recurso específico y se refiere a uno o más controles MAS TRMG. Un control de las MAS TRMG de enero de 2021 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	AWS Regla de configuración	Directrices
3.3.1	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
5.4.3	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación

ID de control	AWS Regla de configuración	Directrices
		AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.
5.4.3	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	AWS Regla de configuración	Directrices
6.1.1	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.
6.1.2	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	AWS Regla de configuración	Directrices
6.1.4	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
6.1.4	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
6.1.4	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
6.2.1	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
6.3.1	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.
6.4.5	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
6.4.5	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
6.4.5	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
6.4.5	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	AWS Regla de configuración	Directrices
6.4.5	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
6.4.5	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
6.4.5	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	AWS Regla de configuración	Directrices
6.4.5	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
6.4.5	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
6.4.5	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
6.4.5	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
6.4.5	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
6.4.6	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
6.4.6	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
6.4.6	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
6.4.6	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	AWS Regla de configuración	Directrices
6.4.6	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
6.4.6	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
6.4.6	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
6.4.6	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
6.4.6	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
6.4.6	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
6.4.7	api-gw-execution-logging-ha bilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
6.4.7	cloud-trail-cloud-watch-hab ilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
6.4.7	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
6.4.7	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
6.4.7	cloudtrail-s3-dataevents-en abled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
6.4.7	cloudtrail-security-trail-enabled	Esta regla ayuda a garantiza r el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, al comprobar la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
6.4.7	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	AWS Regla de configuración	Directrices
6.4.7	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
6.4.7	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
6.4.7	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
6.4.7	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
6.4.7	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
6.4.7	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
6.4.7	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
6.4.7	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	AWS Regla de configuración	Directrices
6.4.8	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
6.4.8	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
6.4.8	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.
6.4.8	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	AWS Regla de configuración	Directrices
6.4.8	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
6.4.8	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
6.4.8	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
6.4.8	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
7.2.1	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
7.2.1	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
7.4.1	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
7.4.1	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	AWS Regla de configuración	Directrices
7.4.1	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
7.4.1	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
7.4.1	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	AWS Regla de configuración	Directrices
7.4.1	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
7.5.5	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.
7.5.5	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
7.5.5	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.
7.5.5	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
7.5.5	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
7.5.5	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	AWS Regla de configuración	Directrices
7.5.5	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
7.5.5	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
7.5.5	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
7.5.5	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.
7.5.7	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
7.5.7	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
7.5.7	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
7.5.7	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
7.5.7	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
7.5.7	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
7.5.7	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
7.5.7	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilad os proporcionan información detallada sobre las solicitud es enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
7.5.7	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
7.5.7	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.
7.5.7	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
7.5.7	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
8.1.1	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
8.1.1	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.
8.1.1	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	AWS Regla de configuración	Directrices
8.1.1	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
8.1.1	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
8.1.1	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	AWS Regla de configuración	Directrices
8.1.1	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
8.1.1	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resilienc ia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	AWS Regla de configuración	Directrices
8.1.2	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	AWS Regla de configuración	Directrices
8.1.2	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
8.1.2	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
8.1.2	opensearch-data-node-fault-tolerancia	Amazon OpenSearch Service (OpenSearch Servicio) requiere al menos tres nodos de datos para una alta disponibilidad y tolerancia a errores. La implementación de un dominio OpenSearch de servicio con al menos tres nodos de datos garantiza las operaciones del clúster en caso de que un nodo falle.

ID de control	AWS Regla de configuración	Directrices
8.1.2	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.
8.1.3	autoscaling-group-elb-healt hcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibi lidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	AWS Regla de configuración	Directrices
8.1.3	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.
8.1.3	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
8.1.3	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
8.4.1	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	AWS Regla de configuración	Directrices
8.4.1	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
8.4.1	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	AWS Regla de configuración	Directrices
8.4.1	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
8.4.1	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporcio na capacidad adicional y dedicada para las operacion es de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	AWS Regla de configuración	Directrices
8.4.1	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
8.4.1	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
8.4.1	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatiz adas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantán ea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
8.4.1	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	AWS Regla de configuración	Directrices
8.4.1	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
8.4.1	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	AWS Regla de configuración	Directrices
8.4.2	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.
8.4.2	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
8.4.2	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.
8.4.2	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
8.4.2	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporcio na capacidad adicional y dedicada para las operacion es de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.
8.4.2	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administr ación de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
8.4.2	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	AWS Regla de configuración	Directrices
8.4.2	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
8.4.2	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.
8.4.2	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
8.4.2	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.
8.4.4	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
8.5.4	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en la infraestructura, Amazon RDS realiza una conmutación por error automática a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	AWS Regla de configuración	Directrices
8.5.4	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
9.1.1	ec2- instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
9.1.1	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	AWS Regla de configuración	Directrices
9.1.1	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
9.1.1	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
9.1.1	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
9.1.1	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
9.1.1	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
9.1.1	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
9.1.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegi o y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
9.1.1	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
9.1.1	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
9.1.1	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
9.1.1	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
9.1.1	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
9.1.1	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
9.1.1	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
9.1.1	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
9.1.1	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS
9.1.1	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	AWS Regla de configuración	Directrices
9.1.1	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
9.1.1	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check . Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	AWS Regla de configuración	Directrices
9.1.1	secretsmanager-secret-periodic-rotation	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitad a la rotación periódica. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela. El valor predeterm inado es 90 días.
9.1.1	secretsmanager-secret-unused	Si existen credenciales no utilizadas en AWS Secrets Manager, debe deshabilitar la opción and/or Eliminar las credenciales, ya que esto podría infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedForDays (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
9.1.2	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
9.1.2	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
9.1.2	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
9.1.2	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
9.1.2	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
9.1.2	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
9.1.3	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
9.1.3	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
9.1.3	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
9.1.3	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
9.1.3	cloudtrail-s3-dataevents-en abled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
9.1.3	cloudtrail-security-trail-enabled	Esta regla ayuda a garantiza r el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.
9.1.3	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	AWS Regla de configuración	Directrices
9.1.3	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
9.1.3	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	AWS Regla de configuración	Directrices
9.1.3	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
9.1.3	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
9.1.3	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
9.1.3	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
9.1.3	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
9.1.3	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
9.1.3	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
9.1.3	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
9.1.3	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	AWS Regla de configuración	Directrices
9.1.4	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
9.1.5	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	AWS Regla de configuración	Directrices
9.1.5	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
9.1.5	root-account-hardware-mfa-h abilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegi os. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
9.1.5	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
9.1.6	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
9.1.7	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
9.1.7	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
9.1.7	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
9.1.7	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
9.1.7	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
9.1.7	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
9.2.1	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
9.2.1	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
9.2.1	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
9.2.1	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
9.2.1	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	AWS Regla de configuración	Directrices
9.2.1	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
9.2.1	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	AWS Regla de configuración	Directrices
9.2.1	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	AWS Regla de configuración	Directrices
9.2.1	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
9.2.1	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
9.2.1	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
9.2.2	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
9.2.2	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
9.2.2	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
9.2.2	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	AWS Regla de configuración	Directrices
9.2.2	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.
9.2.2	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	AWS Regla de configuración	Directrices
9.2.2	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
9.2.2	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
9.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
9.2.2	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
9.2.2	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
9.3.1	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
9.3.1	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
9.3.1	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
9.3.1	opensearch-node-to-node-ver ificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
9.3.1	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
9.3.1	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
9.3.1	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
9.3.1	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
9.3.1	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
9.3.1	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
9.3.1	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
9.3.1	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
9.3.1	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
9.3.1	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
9.3.1	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
10.1.1	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
10.1.1	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
10.1.1	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
10.1.1	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	AWS Regla de configuración	Directrices
10.1.1	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
10.1.1	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
10.1.1	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
10.1.1	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
10.1.1	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
10.1.1	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
10.1.1	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	AWS Regla de configuración	Directrices
10.1.1	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
10.1.1	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
10.1.1	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
10.1.1	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
10.1.1	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
10.1.1	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
10.1.1	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
10.1.1	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitad o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
10.1.1	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
10.1.1	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
10.1.1	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
10.1.1	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	AWS Regla de configuración	Directrices
10.1.1	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
10.1.1	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
10.1.1	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
10.1.1	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
10.1.1	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitad o para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenc iales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
10.1.1	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
10.2.1	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.
10.2.1	cmk-backing-key-rotation-ha bilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	AWS Regla de configuración	Directrices
10.2.1	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
10.2.2	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	AWS Regla de configuración	Directrices
10.2.3	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.
10.2.3	cmk-backing-key-rotation-ha bilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	AWS Regla de configuración	Directrices
10.2.3	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
11.1.1 (a)	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExp iration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (a)	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
11.1.1 (a)	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
11.1.1 (a)	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (a)	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
11.1.1 (a)	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (a)	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
11.1.1 (a)	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
11.1.1 (a)	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (a)	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
11.1.1 (b)	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
11.1.1 (b)	autoscaling-launch-config-p ublic-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidore s.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.
11.1.1 (b)	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
11.1.1 (b)	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
11.1.1 (b)	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.1.1 (b)	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.1.1 (b)	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
11.1.1 (b)	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
11.1.1 (b)	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearc h Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearc h servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
11.1.1 (b)	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.1.1 (b)	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
11.1.1 (b)	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.
11.1.1 (b)	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitada s a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
11.1.1 (b)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
11.1.1 (b)	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
11.1.1 (b)	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
11.1.1 (b)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
11.1.1 (b)	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
11.1.1 (b)	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
11.1.1 (b)	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
11.1.1 (b)	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
11.1.1 (b)	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
11.1.1 (b)	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	AWS Regla de configuración	Directrices
11.1.1 (b)	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
11.1.3	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.1.3	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
11.1.3	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
11.1.3	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	AWS Regla de configuración	Directrices
11.1.3	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.1.3	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
11.1.3	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	AWS Regla de configuración	Directrices
11.1.3	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.
11.1.3	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
11.1.3	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	AWS Regla de configuración	Directrices
11.1.3	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	AWS Regla de configuración	Directrices
11.1.3	emr-kerberos-enabled	Los permisos y autorizac iones de acceso se pueden administrar e incorporar con los principios de privilegi o mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principal es. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El KDC mantiene una base de datos de las entidades principal es dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principal es.

ID de control	AWS Regla de configuración	Directrices
11.1.3	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones . Esta regla le permite establecer el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
11.1.3	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	AWS Regla de configuración	Directrices
11.1.3	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionad as en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establece r el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
11.1.3	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
11.1.3	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
11.1.3	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
11.1.3	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
11.1.3	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
11.1.3	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
11.1.3	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
11.1.3	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñ as y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credencia les, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
11.1.3	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidente s de cuentas compromet idas y evitar que usuarios no autorizados accedan a los datos confidenciales.
11.1.3	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.1.3	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.1.3	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
11.1.3	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
11.1.3	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	AWS Regla de configuración	Directrices
11.1.3	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS
11.1.3	habilitado para s3 bucket-se rver-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
11.1.3	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.1.3	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
11.1.3	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
11.1.3	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
11.1.3	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
11.2.1	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
11.2.2	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	AWS Regla de configuración	Directrices
11.2.2	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.2.2	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.2.2	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
11.2.2	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
11.2.2	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	AWS Regla de configuración	Directrices
11.2.2	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.2.2	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
11.2.2	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
11.2.2	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.
11.2.2	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
11.2.2	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
11.2.2	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
11.2.2	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
11.2.2	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
11.2.2	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
11.2.2	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
11.2.2	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
11.2.2	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
11.2.2	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
11.2.2	subnet-auto-assign-public-ip-deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.
11.2.2	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
11.2.2	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.
11.2.4	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	AWS Regla de configuración	Directrices
11.2.4	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.2.4	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.2.4	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
11.2.4	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicame nte a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
11.2.4	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
11.2.4	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
11.2.4	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
11.2.4	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	AWS Regla de configuración	Directrices
11.2.4	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.
11.2.4	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
11.2.4	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
11.2.4	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
11.2.4	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
11.2.4	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
11.2.4	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
11.2.4	s3- bucket-public-write-prohibi ted	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
11.2.4	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
11.2.4	subnet-auto-assign-public-ip-deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
11.2.4	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
11.2.4	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
11.3.1	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.
11.3.5	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
11.3.5	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
11.3.5	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
11.3.5	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
11.4.2	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
11.4.2	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.
11.4.2	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	AWS Regla de configuración	Directrices
11.4.2	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
11.5.2	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
12.1.1	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
12.1.1	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
12.1.1	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
12.1.1	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
12.2.2	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
12.2.2	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	AWS Regla de configuración	Directrices
12.2.2	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
12.2.2	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrai l registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	AWS Regla de configuración	Directrices
12.2.2	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
12.2.2	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
12.2.2	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	AWS Regla de configuración	Directrices
12.2.2	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.
12.2.2	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
12.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
12.2.2	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
12.2.2	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
12.2.2	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
12.2.2	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
12.2.2	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	AWS Regla de configuración	Directrices
12.2.2	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona informaci ón detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
12.2.4	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
12.2.4	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
12.2.5	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	AWS Regla de configuración	Directrices
12.2.5	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
12.2.5	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
12.2.5	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
12.3.2	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de cibersegu ridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automátic o para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
12.3.2	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
12.3.2	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
14.1.2	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
14.1.2	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
14.1.2	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
14.1.2	opensearch-node-to-node-ver ificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearc h de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicac iones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
14.1.2	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
14.1.2	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
14.1.2	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
14.1.2	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
14.1.2	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
14.1.3	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	AWS Regla de configuración	Directrices
14.1.3	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
14.1.3	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	AWS Regla de configuración	Directrices
14.1.3	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS
14.2.2	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	AWS Regla de configuración	Directrices
14.2.2	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
14.2.2	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
14.2.2	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	AWS Regla de configuración	Directrices
14.2.2	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
14.2.2	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
14.2.2	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
14.2.2	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
14.2.2	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
14.2.2	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	AWS Regla de configuración	Directrices
14.2.2	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
14.2.2	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
14.2.6	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
14.2.6	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
14.2.6	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
14.2.6	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
14.2.6	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
14.2.6	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitad o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
14.2.6	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
14.2.6	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para MAS TRMG.

Prácticas operativas recomendadas para el monitoreo

Este paquete de conformidad contiene AWS Config reglas basadas en la supervisión interna AWS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para la supervisión.

Prácticas operativas recomendadas para NBC TRMG

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el marco de directrices de gestión de riesgos tecnológicos (TRM) del Banco Nacional de Camboya (NBC) y las reglas de Config AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a una o más directrices TRM de NBC. Una directriz del NBC TRM puede estar relacionada con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones de los controles incluidos en el marco normativo Technology Risk Management (TRM) del National Bank of Cambodia (NBC), al que se puede acceder aquí: National Bank of Cambodia: Technology Risk Management Guidelines.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	proceso sistemático de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implementación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterminados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de		usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso; - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	api-gw-execution-l ogging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	cloud-trail-cloud-watch-habilitada para guardar registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso; - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	cloudwatch-alarm-a ction-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluació n. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso; - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemático de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implementación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterminados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	wafv2-logging-enabled	Para facilitar el registro y la supervisión de su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso; - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	account-part-of-or ganizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantiza r que las cuentas cumplan con las normas. La falta de gobernanza centraliz ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEncryptFrom)

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemático de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implementación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterminados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemático de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implementación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterminados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemático de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implementación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterminados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1 (d)	d) Entre los controles importantes que deben tenerse en cuenta figuran: - Un proceso sistemáti co de solicitud y autorización de la creación del usuario IDs y la matriz de control de acceso; - Realizar una evaluación de riesgos y conceder los derechos de acceso en función de los mismos. - Implement ación de un control de acceso basado en roles diseñado para garantizar una separación efectiva de funciones - Cambiar los nombres de usuario predeterm inados, and/or las contraseñas de los sistemas y prohibir compartir los usuarios IDs y las contraseñas de las cuentas genéricas - Modificación de los derechos de	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y transmitidos a Amazon CloudWatc h Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditoría s de seguridad y acceso, y pueden ayudar a diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	acceso siempre que haya un cambio de función o responsabilidad y eliminación de los derechos de acceso al cesar el empleo o contrato - Procesos para notificar oportunamente a la función de seguridad de la información sobre las incorporaciones, eliminaciones y cambios de funciones de usuarios - Conciliación periódica del usuario IDs en un sistema y los usuarios reales deben tener acceso y eliminar todo lo innecesario IDs, si lo hubiera: auditar, registrar y monitorear el acceso a los activos de TI por parte de todos los usuarios y - Considerar la posibilidad IDs de desactivar a los usuarios de aplicaciones críticas		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	que se encuentran de licencia prolongada		
3.1.1(f)	f) A efectos de rendición de cuentas, asegúrese de que los usuarios y los activos de TI estén identific ados de forma única y de que sus acciones sean auditables.	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(f)	f) A efectos de rendición de cuentas, asegúrese de que los usuarios y los activos de TI estén identific ados de forma única y de que sus acciones sean auditables.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(f)	f) A efectos de rendición de cuentas, asegúrese de que los usuarios y los activos de TI estén identific ados de forma única y de que sus acciones sean auditables.	opensearch-audit-l ogging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearc h de Amazon Service. El registro de auditoría le permite realizar un seguimien to de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexació n y las consultas de búsqueda entrantes.
3.1.1(f)	f) A efectos de rendición de cuentas, asegúrese de que los usuarios y los activos de TI estén identific ados de forma única y de que sus acciones sean auditables.	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(f)	f) A efectos de rendición de cuentas, asegúrese de que los usuarios y los activos de TI estén identific ados de forma única y de que sus acciones sean auditables.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(f)	f) A efectos de rendición de cuentas, asegúrese de que los usuarios y los activos de TI estén identific ados de forma única y de que sus acciones sean auditables.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(f)	f) A efectos de rendición de cuentas, asegúrese de que los usuarios y los activos de TI estén identific ados de forma única y de que sus acciones sean auditables.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y transmitidos a Amazon CloudWatc h Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditoría s de seguridad y acceso, y pueden ayudar a diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Establecer controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado en función de «o need-to-haveneed-to-do» - Mantener un registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se recopilan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	códigos de acceso privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube. AWS Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	root-account-hardware-mfa-activado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	cloud-trail-cloud-watch-registros activados	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Establecer controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado en función de «o need-to-haveneed-to-do» - Mantener un registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se recopilan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	códigos de acceso privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Es	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	necesario tener en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Establecer controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado en función de «o need-to-haveneed-to-do» - Mantener un registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se recopilan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	códigos de acceso privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Establecer controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado en función de «o need-to-haveneed-to-do» - Mantener un registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se recopilan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	códigos de acceso privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEncryptFrom)

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Es	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	necesario tener en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Establecer controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado en función de «o need-to-haveneed-to-do» - Mantener un registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se recopilan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	códigos de acceso privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administradores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operaciones críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financieros que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegios. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisión y registrar todas sus actividades en los sistemas, ya que tiene conocimientos internos y los recursos necesarios para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Deben	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	tenerse en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Instituir controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado «o need-to-haveneed-to-do» - Mantener el registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se capturan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los códigos de acceso		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1(h)	h) Los administr adores de sistemas, los responsables de seguridad, los programadores y el personal que realiza operacion es críticas poseen invariablemente la capacidad de infligir graves daños a los sistemas financier os que mantienen u operan en virtud de sus funciones laborales y de su acceso con privilegi os. El personal con derechos de acceso elevados al sistema debe estar sometido a una rigurosa supervisi ón y registrar todas sus actividades en los sistemas, ya que tiene conocimie ntos internos y los recursos necesario s para eludir los controles de los sistemas y los procedimientos de seguridad. Es	efs-encrypted-check	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	necesario tener en cuenta algunas de las prácticas de control y seguridad que se enumeran a continuación: - Implementar una autenticación de dos factores para los usuarios privilegiados - Establecer controles estrictos sobre el acceso remoto de los usuarios privilegiados - Conceder el acceso privilegiado en función de «o need-to-haveneed-to-do» - Mantener un registro de auditoría de las actividades del sistema realizadas por los usuarios privilegiados - Garantizar que los usuarios privilegiados no tengan acceso a los registros del sistema en los que se recopilan sus actividades - Realizar auditorías o revisiones de gestión periódicas de los registros - Prohibir compartir los		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	códigos de acceso privilegiados IDs y sus códigos de acceso - Impedir que los proveedores y contratistas obtengan acceso privilegiado a los sistemas sin una estrecha supervisión y supervisión y _ Proteger los datos de respaldo contra el acceso no autorizado		
3.1.2(a)	a) El BFI debería instalar dispositivos de seguridad de red, como firewalls, software antivirus y antimalware, así como sistemas de detección y prevención de intrusiones, en los puntos críticos de su infraestructura de TI, para proteger los perímetros de la red.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(a)	a) El BFI debería instalar dispositivos de seguridad de red, como firewalls , software antivirus y antimalware, así como sistemas de detección y prevenció n de intrusiones, en los puntos críticos de su infraestructura de TI, para proteger los perímetros de la red.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(a)	a) El BFI debería instalar dispositivos de seguridad de red, como firewalls , software antivirus y antimalware, así como sistemas de detección y prevenció n de intrusiones, en los puntos críticos de su infraestructura de TI, para proteger los perímetros de la red.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	alb-http-drop-invalid-habilitado para encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implement arse controles para garantizar la seguridad de la información en las redes y la protecció n de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáti cas cuando proceda - Deben establecerse controles especiale s para salvaguardar la confidencialidad e integridad de los datos que atraviesa n redes públicas o redes inalámbricas y para proteger los sistemas y aplicacio nes conectados	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implement arse controles para garantizar la seguridad de la información en las redes y la protecció n de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáti cas cuando proceda - Deben establecerse controles especiale s para salvaguardar la confidencialidad e integridad de los datos que atraviesa n redes públicas o redes inalámbricas y para proteger los sistemas y aplicacio nes conectados	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implement arse controles para garantizar la seguridad de la información en las redes y la protecció n de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáti cas cuando proceda - Deben establecerse controles especiale s para salvaguardar la confidencialidad e integridad de los datos que atraviesa n redes públicas o redes inalámbricas y para proteger los sistemas y aplicacio nes conectados	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		Amazon VPC para gestionar correctamente el acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		deben asignarse a una VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	s3- account-level-public-access -bloquea-periódico	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2(c)	c) Deben implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos: - Deben establecerse las responsabilidades y los procedimientos para la gestión de los equipos de redes - La responsabilidad operativa de las redes debe separarse de las operaciones informáticas cuando proceda - Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectados	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	(se deben incluir protocolos de cifrado de red cuando se conecte a sistemas o redes que no sean de confianza). - Se deben aplicar los procedimientos de registro y supervisión adecuados para permitir la trazabilidad y la detección de las acciones que puedan afectar o sean relevantes para la seguridad de la información - Las actividades de gestión deben coordinarse estrechamente tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información - Los sistemas de la red deben autenticarse - Deben restringirse las conexiones de		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	sistemas no confiables a la red		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certifica dos deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExp iration (valor de prácticas recomenda das de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	alb-http-drop-inva lid-habilitado para encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2 (e)	e) Los servicios de red pueden abarcar desde un simple ancho de banda no administrado hasta servicios sofistica dos como VPN, voz sobre IP, VSAT, etc. Las características de seguridad de los servicios de red deberían ser: - La tecnología aplicada a la seguridad de los servicios de red, como la autentica ción, el cifrado y los controles de conexión de red. - Los parámetros técnicos necesarios para una conexión segura con los servicios de red acordes a la normativa de seguridad y conexión de red. - Los procedimientos para el uso del servicio de red con el fin de restringir el acceso a los servicios o aplicaciones de red,	elbv2- acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cuando sea necesario .		
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	alb-http-drop-invalid-habilitado para encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
3.1.3 (e)	e) Utilice el cifrado para proteger los canales de comunicación entre el dispositivo de acceso remoto y la institución con el fin de restringir los riesgos relacionados con la suplantación de la red.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizada s a través del acceso remoto	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizada s a través del acceso remoto	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (g)	g) Mantenimiento de registros para las comunicaciones de acceso remoto. Los registros deben incluir la fecha, la hora, el usuario, la ubicación del usuario, la duración y el propósito de todos los accesos remotos, incluidas todas las actividades realizadas a través del acceso remoto	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (i)	i) Implementación de un proceso de autenticación de dos factores para el acceso remoto (por ejemplo, una tarjeta de token basada en un PIN con un generador de contraseñas aleatorias de un solo uso o una PKI basada en tokens)	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (i)	i) Implementación de un proceso de autenticación de dos factores para el acceso remoto (por ejemplo, una tarjeta de token basada en un PIN con un generador de contraseñas aleatorias de un solo uso o una PKI basada en tokens)	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (i)	i) Implementación de un proceso de autenticación de dos factores para el acceso remoto (por ejemplo, una tarjeta de token basada en un PIN con un generador de contraseñas aleatorias de un solo uso o una PKI basada en tokens)	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3 (i)	i) Implementación de un proceso de autenticación de dos factores para el acceso remoto (por ejemplo, una tarjeta de token basada en un PIN con un generador de contraseñas aleatorias de un solo uso o una PKI basada en tokens)	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4 (c) (e)	c) El proceso de gestión de parches debe incluir aspectos como: - Determinar los métodos para obtener y validar los parches a fin de garantizar que el parche proviene de una fuente autorizada - Identificar las vulnerabilidades que son aplicables a las aplicaciones y los sistemas utilizados por la organización - Evaluar el impacto empresarial de la implementación de parches (o no implementar un parche en particular) - Garantizar que los parches se prueben - Describir los métodos para implementar los parches, por ejemplo, automáticamente - Informar sobre el estado del despliegue de los parches en toda la organización y - Incluir los	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	métodos para hacer frente a la implementación fallida de un parche (por ejemplo, la redistribución del parche). e) BFIs debería implementar herramientas automatizadas de administración de parches y herramientas de actualización de software para todos los sistemas para los que dichas herramientas estén disponibles y sean seguras		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4 (c) (e)	c) El proceso de gestión de parches debe incluir aspectos como: - Determinar los métodos para obtener y validar los parches a fin de garantizar que el parche proviene de una fuente autorizada - Identificar las vulnerabilidades que son aplicables a las aplicaciones y los sistemas utilizados por la organización - Evaluar el impacto empresarial de la implementación de parches (o no implementar un parche en particular) - Garantizar que los parches se prueben - Describir los métodos para implementar los parches, por ejemplo, automáticamente - Informar sobre el estado del despliegue de los parches en toda la organización y - Incluir los	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	métodos para hacer frente a la implementación fallida de un parche (por ejemplo, la redistribución del parche). e) BFIs debería implementar herramientas automatizadas de administración de parches y herramientas de actualización de software para todos los sistemas para los que dichas herramientas estén disponibles y sean seguras		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4 (c) (e)	c) El proceso de gestión de parches debe incluir aspectos como: - Determinar los métodos para obtener y validar los parches a fin de garantizar que el parche proviene de una fuente autorizada - Identificar las vulnerabilidades que son aplicables a las aplicaciones y los sistemas utilizados por la organización - Evaluar el impacto empresarial de la implementación de parches (o no implementar un parche en particular) - Garantizar que los parches se prueben - Describir los métodos para implementar los parches, por ejemplo, automáticamente - Informar sobre el estado del despliegue de los parches en toda la organización y - Incluir los	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	métodos para hacer frente a la implementación fallida de un parche (por ejemplo, la redistribución del parche). e) BFIs debería implementar herramientas automatizadas de administración de parches y herramientas de actualización de software para todos los sistemas para los que dichas herramientas estén disponibles y sean seguras		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4 (c) (e)	c) El proceso de gestión de parches debe incluir aspectos como: - Determinar los métodos para obtener y validar los parches a fin de garantizar que el parche proviene de una fuente autorizada - Identificar las vulnerabilidades que son aplicables a las aplicaciones y los sistemas utilizados por la organización - Evaluar el impacto empresarial de la implementación de parches (o no implementar un parche en particular) - Garantizar que los parches se prueben - Describir los métodos para implementar los parches, por ejemplo, automáticamente - Informar sobre el estado del despliegue de los parches en toda la organización y - Incluir los	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	métodos para hacer frente a la implementación fallida de un parche (por ejemplo, la redistribución del parche). e) BFIs debería implementar herramientas automatizadas de administración de parches y herramientas de actualización de software para todos los sistemas para los que dichas herramientas estén disponibles y sean seguras		las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4 (c) (e)	c) El proceso de gestión de parches debe incluir aspectos como: - Determinar los métodos para obtener y validar los parches a fin de garantizar que el parche proviene de una fuente autorizada - Identificar las vulnerabilidades que son aplicables a las aplicaciones y los sistemas utilizados por la organización - Evaluar el impacto empresarial de la implementación de parches (o no implementar un parche en particular) - Garantizar que los parches se prueben - Describir los métodos para implementar los parches, por ejemplo, automáticamente - Informar sobre el estado del despliegue de los parches en toda la organización y - Incluir los	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	métodos para hacer frente a la implementación fallida de un parche (por ejemplo, la redistribución del parche). e) BFIs debería implementar herramientas automatizadas de administración de parches y herramientas de actualización de software para todos los sistemas para los que dichas herramientas estén disponibles y sean seguras		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4 (c) (e)	c) El proceso de gestión de parches debe incluir aspectos como: - Determinar los métodos para obtener y validar los parches para garantizar que proceden de una fuente autorizada - Identificar las vulnerabilidades aplicables a las aplicaciones y sistemas utilizados por la organización - Evaluar el impacto empresarial de implementar parches (o no implementar un parche en particular) - Garantizar que los parches se prueban - Describir los métodos para implementar los parches, por ejemplo de forma automática - Informar sobre el estado del despliegue de los parches en toda la organización e incluir los métodos para hacer frente a	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	la implementación fallida de un parche (por ejemplo, la redistribución del parche). e) BFIs debería implement ar herramientas automatizadas de administración de parches y herramien tas de actualización de software para todos los sistemas para los que dichas herramientas estén disponibles y sean seguras		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (d) (e)	d) La gestión adecuada de las claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir las claves criptográficas. e) Todas las claves criptográficas deben protegerse contra la modificación y la pérdida. Además, las claves secretas y privadas deben protegerse contra el uso no autorizado y la divulgación. El equipo utilizado para generar, almacenar y archivar las claves debe estar protegido físicamente.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (d) (e)	d) La gestión adecuada de las claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir las claves criptográficas. e) Todas las claves criptográficas deben protegerse contra la modificación y la pérdida. Además, las claves secretas y privadas deben protegerse contra el uso no autorizado y la divulgación. El equipo utilizado para generar, almacenar y archivar las claves debe estar protegido físicamente.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (d) (e)	d) La gestión adecuada de las claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir las claves criptográficas. e) Todas las claves criptográficas deben protegerse contra la modificación y la pérdida. Además, las claves secretas y privadas deben protegerse contra el uso no autorizado y la divulgación. El equipo utilizado para generar, almacenar y archivar las claves debe estar protegido físicamente.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (d) (e)	d) La gestión adecuada de las claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir las claves criptográficas. e) Todas las claves criptográficas deben protegerse contra la modificación y la pérdida. Además, las claves secretas y privadas deben protegerse contra el uso no autorizado y la divulgación. El equipo utilizado para generar, almacenar y archivar las claves debe estar protegido físicamente.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar, kms:ReEncryptFrom)

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (f)	f) Un sistema de administración de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para: - generar claves para diferentes sistemas criptográficos y diferentes aplicaciones; emitir y obtener certificados de clave pública; - distribuir claves a las entidades previstas, lo que incluye la forma en que se deben activar las claves cuando se reciben; - almacenar las claves, lo que incluye la forma en que los usuarios autorizados obtienen acceso a las claves; - cambiar o actualizar las claves, lo que incluye las normas sobre cuándo deben cambiarse las claves y cómo se hará; - gestionar las claves compromet	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	idas; - revocar claves, lo que incluye cómo deben revocarse o desactivarse las claves (por ejemplo, cuando las claves se han visto compromet idas o cuando un usuario abandona una organización, en cuyo caso, las claves también deben archivars e); - recuperar las claves perdidas o corruptas; - hacer copias de seguridad o archivar las claves; - destruir las claves; y - registrar y auditar las actividades relaciona das con la administr ación de claves.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (f)	f) Un sistema de administración de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para: - generar claves para diferentes sistemas criptográficos y diferentes aplicaciones; emitir y obtener certificados de clave pública; - distribuir claves a las entidades previstas, lo que incluye la forma en que se deben activar las claves cuando se reciben; - almacenar las claves, lo que incluye la forma en que los usuarios autorizados obtienen acceso a las claves; - cambiar o actualizar las claves, lo que incluye las normas sobre cuándo deben cambiarse las claves y cómo se hará; - gestionar las claves compromet	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	idas; - revocar claves, lo que incluye cómo deben revocarse o desactivarse las claves (por ejemplo, cuando las claves se han visto compromet idas o cuando un usuario abandona una organización, en cuyo caso, las claves también deben archivars e); - recuperar las claves perdidas o corruptas; - hacer copias de seguridad o archivar las claves; - destruir las claves; y - registrar y auditar las actividades relaciona das con la administr ación de claves.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (f)	f) Un sistema de administración de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para: - generar claves para diferentes sistemas criptográficos y diferentes aplicaciones; emitir y obtener certificados de clave pública; - distribuir claves a las entidades previstas, lo que incluye la forma en que se deben activar las claves cuando se reciben; - almacenar las claves, lo que incluye la forma en que los usuarios autorizados obtienen acceso a las claves; - cambiar o actualizar las claves, lo que incluye las normas sobre cuándo deben cambiarse las claves y cómo se hará; - gestionar las claves compromet	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	idas; - revocar claves, lo que incluye cómo deben revocarse o desactivarse las claves (por ejemplo, cuando las claves se han visto compromet idas o cuando un usuario abandona una organización, en cuyo caso, las claves también deben archivars e); - recuperar las claves perdidas o corruptas; - hacer copias de seguridad o archivar las claves; - destruir las claves; y - registrar y auditar las actividades relaciona das con la administr ación de claves.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (f)	f) Un sistema de administración de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para: - generar claves para diferentes sistemas criptográficos y diferentes aplicaciones; emitir y obtener certificados de clave pública; - distribuir claves a las entidades previstas, lo que incluye la forma en que se deben activar las claves cuando se reciben; - almacenar las claves, lo que incluye la forma en que los usuarios autorizados obtienen acceso a las claves; - cambiar o actualizar las claves, lo que incluye las normas sobre cuándo deben cambiarse las claves y cómo se hará; - gestionar las claves compromet	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	idas; - revocar claves, lo que incluye cómo deben revocarse o desactivarse las claves (por ejemplo, cuando las claves se han visto compromet idas o cuando un usuario abandona una organización, en cuyo caso, las claves también deben archivars e); - recuperar las claves perdidas o corruptas; - hacer copias de seguridad o archivar las claves; - destruir las claves; y - registrar y auditar las actividades relaciona das con la administr ación de claves.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (f)	f) Un sistema de administración de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para: - generar claves para diferentes sistemas criptográficos y diferentes aplicaciones; emitir y obtener certificados de clave pública; - distribuir claves a las entidades previstas, lo que incluye la forma en que se deben activar las claves cuando se reciben; - almacenar las claves, lo que incluye la forma en que los usuarios autorizados obtienen acceso a las claves; - cambiar o actualizar las claves, lo que incluye las normas sobre cuándo deben cambiarse las claves y cómo se hará; - gestionar las claves compromet	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	idas; - revocar claves, lo que incluye cómo deben revocarse o desactivarse las claves (por ejemplo, cuando las claves se han visto compromet idas o cuando un usuario abandona una organización, en cuyo caso, las claves también deben archivars e); - recuperar las claves perdidas o corruptas; - hacer copias de seguridad o archivar las claves; - destruir las claves; y - registrar y auditar las actividades relaciona das con la administr ación de claves.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (f)	f) Un sistema de administración de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para: - generar claves para diferentes sistemas criptográ ficos y diferentes aplicaciones; emitir y obtener certificados de clave pública; - distribuir claves a las entidades previstas, lo que incluye la forma en que se deben activar las claves cuando se reciben; - almacenar las claves, lo que incluye la forma en que los usuarios autorizados obtienen acceso a las claves; - cambiar o actualizar las claves, lo que incluye las normas sobre cuándo deben cambiarse las claves y cómo se hará; - gestionar las claves compromet	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	idas; - revocar claves, lo que incluye cómo deben revocarse o desactivarse las claves (por ejemplo, cuando las claves se han visto compromet idas o cuando un usuario abandona una organización, en cuyo caso, las claves también deben archivars e); - recuperar las claves perdidas o corruptas; - hacer copias de seguridad o archivar las claves; - destruir las claves; y - registrar y auditar las actividades relaciona das con la administr ación de claves.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5 (f)	f) Un sistema de administración de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para: - generar claves para diferentes sistemas criptográficos y diferentes aplicaciones; emitir y obtener certificados de clave pública; - distribuir claves a las entidades previstas, lo que incluye la forma en que se deben activar las claves cuando se reciben; - almacenar las claves, lo que incluye la forma en que los usuarios autorizados obtienen acceso a las claves; - cambiar o actualizar las claves, lo que incluye las normas sobre cuándo deben cambiarse las claves y cómo se hará; - gestionar las claves compromet	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	idas; - revocar claves, lo que incluye cómo deben revocarse o desactivarse las claves (por ejemplo, cuando las claves se han visto compromet idas o cuando un usuario abandona una organización, en cuyo caso, las claves también deben archivars e); - recuperar las claves perdidas o corruptas; - hacer copias de seguridad o archivar las claves; - destruir las claves; y - registrar y auditar las actividades relaciona das con la administr ación de claves.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.6 (a)	a) El BFI debería utilizar una combinación de herramientas automatizadas y técnicas manuales para realizar una prueba de vulnerabilidades (VA) exhaustiva de forma periódica. En el caso de los sistemas externos basados en la web, el alcance de la VA debe incluir vulnerabilidades web comunes, como la inyección SQL y las secuencias de comandos entre sitios.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.6 (a)	a) El BFI debería utilizar una combinación de herramientas automatizadas y técnicas manuales para realizar una prueba de vulnerabilidades (VA) exhaustiva de forma periódica. En el caso de los sistemas externos basados en la web, el alcance de la VA debe incluir vulnerabilidades web comunes, como la inyección SQL y las secuencias de comandos entre sitios.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.6 (a)	a) El BFI debería utilizar una combinación de herramientas automatizadas y técnicas manuales para realizar una prueba de vulnerabilidades (VA) exhaustiva de forma periódica. En el caso de los sistemas externos basados en la web, el alcance de la VA debe incluir vulnerabilidades web comunes, como la inyección SQL y las secuencias de comandos entre sitios.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.6 (c)	c) El BFI debería establecer un proceso para subsanar los problemas identificados en las pruebas de vulnerabilidades y penetración (VA y PT) y, posteriormente, revalidar la solución para validar que las brechas se hayan abordado por completo.	vuln-mitigated-accepted(Verificación del proceso)	Asegúrese de que las vulnerabilidades recientemente identificadas se corrijan o documenten como riesgos aceptados. Las vulnerabilidades deben remediarse o aceptarse como riesgos de acuerdo con los requisitos de cumplimiento de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.6 (f)	f) La función de seguridad debería proporcionar actualizaciones sobre el estado del número de vulnerabilidades críticas y no mitigadas para cada departamento o división, y planificar su mitigación por parte de la alta dirección de forma periódica	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.8	Formación y concienciación de los usuarios	security-awareness-program-exists(Verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrai l entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	efs-encrypted-check	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	elasticsearch-encr ypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	opensearch-encrypt ed-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	Habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	sagemaker-notebook -instance-kms-conf igurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	rds-snapshot-encry pted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	api-gw-cache-enabl ed-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	dynamodb-table-enc rypted-kms	Asegúrese de que el cifrado esté habilitad o para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenc iales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitad o para su clúster de Amazon Redshift. Puesto que puede haber datos confidenc iales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.10 (b)	b) La informaci ón confidencial, como la documenta ción del sistema, el código fuente de la aplicación y los datos de las transacci ones de producción debería estar sujeta a controles más exhaustivos para evitar su alteració n (por ejemplo, comprobadores de integridad o hashes criptográ ficos). Además, las políticas deberían minimizar la distribuc ión de la información confidencial, incluidas las copias impresas que contengan la información.	secretsmanager-usi ng-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenc iales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicacio nes afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debería realizar copias de seguridad de los sistemas o aplicaciones afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicaciones afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicacio nes afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicacio nes afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicacio nes afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicacio nes afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicacio nes afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicacio nes afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicacio nes afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (h)	h) Para minimizar los riesgos asociados a los cambios, BFIs debe realizar copias de seguridad de los sistemas o aplicaciones afectados antes del cambio. BFIs debe establecer un plan de reversión para volver a una versión anterior del sistema o de la aplicación en caso de que surja algún problema durante o después de la implementación.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado o para registrar las actividades que se realizan durante el proceso de migración.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado o para registrar las actividades que se realizan durante el proceso de migración.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado o para registrar las actividades que se realizan durante el proceso de migración.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado o para registrar las actividades que se realizan durante el proceso de migración.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1 (k)	k) Los registros de auditoría y seguridad son información útil que facilita las investigaciones y la resolución de problemas. El BFI debe asegurarse de que el instrumento de registro esté habilitado para registrar las actividades que se realizan durante el proceso de migración.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.3 (a)	a) Desarrollar e implementar procesos para prevenir, detectar, analizar y responder a los incidentes de seguridad de la información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.3 (a)	a) Desarrollar e implementar procesos para prevenir, detectar, analizar y responder a los incidentes de seguridad de la información.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores importantes relacionados con el mantenimiento de una alta disponibilidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	dynamodb-pitr-enab led	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantiza r que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores importantes relacionados con el mantenimiento de una alta disponibilidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	elb-deletion-prote ction-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protecció n contra borrado. Utilice esta caracterí stica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibi lidad de sus aplicacio nes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	vpc-vpn-2-tunnels-up	Se pueden implement ar túneles Site-to-S ite VPN redundant es para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectivi dad en caso de que una de las conexione s Site-to-Site VPN no esté disponibl e. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	elb-cross-zone-loa d-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automátic o de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibi lidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexione s o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	dynamodb-throughpu t-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/ write actividad que puede soportar cada mesa. DynamoDB utiliza esta informaci ón para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalm ente los parámetro s de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
3.3.1 (a)	a) Tenga en cuenta los factores important es relacionados con el mantenimiento de una alta disponibi lidad del sistema, una capacidad adecuada, un rendimiento confiable, un tiempo de respuesta rápido y la escalabilidad como parte del diseño del sistema.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultane idad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (a) (b) (c) (f) (j)	a) Asegúrese de que los registros de acceso de los usuarios estén identificados y registrados de forma única con fines de auditoría y revisión. b) Establezca responsabilidades y medidas de identificación del acceso no autorizado. c) Habilite el registro de auditoría de las actividades del sistema realizadas por los usuarios con privilegios. f) Asegúrese de que se apliquen el registro y la supervisión adecuados para permitir el registro y la detección de las acciones que puedan afectar o resulten relevantes para la seguridad de la información. j) Asegúrese de que el registro de eventos siente las bases para unos sistemas de	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	monitoreo automatizados que sean capaces de generar informes y alertas sobre la seguridad del sistema.		
3.4 (f)	f) Asegúrese de que se aplique un registro y monitoreo adecuado para permitir el archivado y la detección de las acciones que puedan afectar a la seguridad de la información o que sean relevantes para ella.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	wafv2-logging-enab led	Para facilitar el registro y la supervisi ón en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la informaci ón sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	api-gw-execution-l ogging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4 (g)	g) Asegúrese de que los registros de eventos incluyan, cuando proceda: - Usuario IDs - Actividades del sistema - Fechas, hora y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión - Identidad o ubicación del dispositivo si es posible e identific ador del sistema - Registros de intentos de acceso al sistema correctos y rechazado s - Registros de intentos de acceso al sistema correctos y rechazados y a otros recursos - Cambios en la configura ción del sistema - Uso de privilegios - Uso de utilidades y aplicaciones del sistema - Archivos accedidos y tipo de acceso - Direccion es y protocolos de red - Alarmas	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y transmitidos a Amazon CloudWatc h Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditoría s de seguridad y acceso, y pueden ayudar a diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	- planteada por el control de acceso sistema y - Registros de las transacci ones ejecutadas por los usuarios en las aplicaciones y las transacciones de los clientes en línea		
3.6.1 (a) (h)	a) BFIs deben garantizar las medidas de seguridad adecuadas para sus aplicaciones web y adoptar medidas atenuantes razonables frente a los diversos riesgos de seguridad web. h) BFIs deben garantiza r las medidas de seguridad adecuadas para sus aplicacio nes web y adoptar medidas atenuantes razonables contra los diversos riesgos de seguridad web	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (a) (h)	a) BFIs necesitan garantizar las medidas de seguridad adecuadas para sus aplicaciones web y tomar medidas atenuantes razonables frente a los diversos riesgos de seguridad web. h) BFIs necesitan garantizar las medidas de seguridad adecuadas para sus aplicaciones web y tomar medidas atenuantes razonables contra los diversos riesgos de seguridad web	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (b)	b) BFIs necesitan evaluar los requisitos de seguridad asociados a sus sistemas de banca por Internet y otros sistemas relevantes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
3.6.1 (b)	b) BFIs necesitan evaluar los requisitos de seguridad asociados a sus sistemas de banca por Internet y otros sistemas relevantes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	alb-http-to-https-control de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (b)	b) BFIs necesitan evaluar los requisitos de seguridad asociados a sus sistemas de banca por Internet y otros sistemas relevantes y adoptar una solución de cifrado teniendo en cuenta el grado de confidencialidad e integridad requerido.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
3.6.1 (b)	b) BFIs necesitan evaluar los requisitos de seguridad asociados a sus sistemas de banca por Internet y otros sistemas pertinentes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (b)	b) BFIs necesitan evaluar los requisitos de seguridad asociados a sus sistemas de banca por Internet y otros sistemas relevantes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.6.1 (b)	b) BFIs necesitan evaluar los requisitos de seguridad asociados a sus sistemas de banca por Internet y otros sistemas relevantes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (b)	b) BFIs necesitan evaluar los requisito s de seguridad asociados a sus sistemas de banca por Internet y otros sistemas relevantes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (b)	b) BFIs necesitan evaluar los requisitos de seguridad asociados a sus sistemas de banca por Internet y otros sistemas relevantes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.6.1 (b)	b) BFIs necesitan evaluar los requisitos de seguridad asociados a sus sistemas de banca por Internet y otros sistemas relevantes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (b)	b) BFIs necesitan evaluar los requisito s de seguridad asociados a sus sistemas de banca por Internet y otros sistemas relevantes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
3.6.1 (b)	b) BFIs necesitan evaluar los requisito s de seguridad asociados a sus sistemas de banca por Internet y otros sistemas pertinentes y adoptar una solución de cifrado que tenga en cuenta el grado de confidencialidad e integridad requerido.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (d)	d) la BFIs prestación de servicios bancarios por Internet debería responder a condiciones de tráfico y rendimiento del sistema poco habituales y a un aumento repentino de la utilización de los recursos del sistema, lo que podría ser un indicio de un ataque tipo DDoS. Como consecuencia, el éxito de cualquier acción preventiva y reactiva depende de la implementación de las herramientas adecuadas para detectar, supervisar y analizar eficazmente las anomalías en las redes y los sistemas.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (d)	d) la banca BFIs por Internet debería responder a condicion es de tráfico y rendimiento del sistema poco habituales y a un aumento repentino de la utilización de los recursos del sistema, lo que podría ser un indicio de un ataque tipo S. DDo Como consecuencia, el éxito de cualquier acción preventiva y reactiva depende de la implementación de las herramien tas adecuadas para detectar, supervisar y analizar eficazmente las anomalías en las redes y los sistemas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (d)	d) la BFIs banca por Internet debería responder a condicion es de tráfico o rendimiento del sistema inusuales de la red y a un aumento repentino de la utilización de los recursos del sistema, lo que podría ser un indicio de un ataque tipo DDo S. Como consecuencia, el éxito de cualquier acción preventiva y reactiva depende de la implementación de las herramien tas adecuadas para detectar, supervisar y analizar eficazmente las anomalías en las redes y los sistemas.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (d)	d) la BFIs prestación de servicios bancarios por Internet debería responder a condiciones de tráfico y rendimiento del sistema poco habituales y a un aumento repentino de la utilización de los recursos del sistema, lo que podría indicar un ataque tipo S. DDo Como consecuencia, el éxito de cualquier acción preventiva y reactiva depende de la implementación de las herramientas adecuadas para detectar, supervisar y analizar eficazmente las anomalías en las redes y los sistemas.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (d)	d) la BFIs prestación de servicios bancarios por Internet debería responder a las condiciones inusuales de tráfico de la red o al rendimiento del sistema y a un aumento repentino de la utilización de los recursos del sistema, lo que podría ser un indicio de un ataque S. DDo Como consecuencia, el éxito de cualquier acción preventiva y reactiva depende de la implementación de las herramien tas adecuadas para detectar, supervisar y analizar eficazmente las anomalías en las redes y los sistemas.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1 (e)	e) BFIs necesitan evaluar periódica mente las vulnerabi lidades de seguridad de la información y evaluar la eficacia del marco de gestión de riesgos de seguridad de TI existente, realizando todos los ajustes necesarios para garantizar que las vulnerabilidades emergentes se aborden de manera oportuna. Esta evaluación también debe realizarse como parte de cualquier cambio sustancial.	guardduty-non-arch ived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasifica ciones para determina r las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.4 (a) (b)	a) Restrinja el acceso a Internet y separe los sistemas críticos del entorno de TI general. b) Reduzca la superficie expuesta a ataques y las vulnerabilidades.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para NBC TRMG.

Prácticas operativas recomendadas para NERC CIP BCSI

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre las normas de protección de infraestructuras críticas de la Corporación de Confiabilidad Eléctrica de Norteamérica (NERC CIP) para la información sobre cibersistemas (BCSI) de BES, CIP-004-7 y CIP-011-3, y las reglas gestionadas. AWS Config Cada regla de AWS Config se aplica a un AWS recurso específico y se refiere a uno o más controles CIP del NERC aplicables a la BCSI. Un control de NERC CIP puede

estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documenta dos para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identific ados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectiva mente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon. OpenSearch Permite un control de acceso al dominio basado en roles, así como una seguridad a nivel de índices, documentos y campos, la compatibi lidad con OpenSearc h paneles de control multiusuario y la autenticación básica HTTP para Kibana. OpenSearch

ID de control	Descripción del control	AWS Config Regla	Directrices
	y utilizar la BCSI. El acceso aprovisionado debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documentados para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identificados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectivamente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener y utilizar la BCSI. El acceso aprovisionado	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Config Regla	Directrices
	debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documentados para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identificados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectivamente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener y utilizar la BCSI. El acceso aprovisionado	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Config Regla	Directrices
	debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documentados para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identificados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectivamente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener y utilizar la BCSI. El acceso aprovisionado	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
	debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documenta dos para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identific ados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectiva mente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener y utilizar la BCSI. El acceso aprovisionado	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Config Regla	Directrices
	debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documentados para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identificados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectivamente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener y utilizar la BCSI. El acceso aprovisionado	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
	debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documentados para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identificados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectivamente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener y utilizar la BCSI. El acceso aprovisionado	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Config Regla	Directrices
	debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documentados para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identificados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectivamente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener y utilizar la BCSI. El acceso aprovisionado	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
	debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documentados para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identificados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectivamente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener y utilizar la BCSI. El acceso aprovisionado	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
	debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-004-7-R6-Parte 6.1	Cada entidad responsable implementará uno o más programas de administración del acceso documentados para autorizar, verificar y revocar el acceso aprovisionado al BCSI en relación con los “sistemas aplicables” identificados en el cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES), que incluyen colectivamente cada uno de los requisitos aplicables del cuadro R6 de la CIP-004-7 (Gestión del acceso a la información del cibersistema BES). Para que se considere acceso a la BCSI en el contexto de este requisito, una persona tiene la capacidad de obtener y utilizar la BCSI. El acceso aprovisionado	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Config Regla	Directrices
	debe considerarse el resultado de las medidas específic as adoptadas para proporcionar a una persona los medios para acceder a la BCSI (por ejemplo, puede incluir claves físicas o tarjetas de acceso, usuarios y derechos y privilegi os asociados o claves de cifrado). Parte 6.1: Antes del aprovisio namiento, autorizac ión (a menos que ya esté autorizado de conformidad con la parte 4.1.), según sea necesario y lo determine la entidad responsable, excepto en las circunstancias excepcionales del CIP: 6.1.1. Acceso electrónico aprovisio nado a la BCSI electrónica		

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	alb-http-drop-invalid-encabezado activado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	ecr-private-image-scanning-habilitado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identific ar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	ecr-private-tag-immutability-habilitado	Se activa la inmutabilidad de las etiquetas del Elastic Container Repository (ECR) para evitar que se sobrescriban las etiquetas de las imágenes de ECR. Anteriormente, las etiquetas podían sobrescribirse, lo que requería metodologías manuales para identificar de forma exclusiva una imagen.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicac ión segura entre Amazon OpenSearc h y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	opensearch-node-to -node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	Habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	s3- event-notifications-enabled	Las notificaciones de eventos de Amazon S3 pueden alertar al personal pertinente de cualquier modificación accidental o intencionada en los objetos de su bucket. Algunos ejemplos de alertas son: creación de un objeto nuevo, eliminación de objetos, restauración de objetos, objetos perdidos o replicados.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	s3- lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	rds-cluster-default-admin-comprobar	Como los nombres de usuario predeterm inados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de los clústeres de bases de datos de Amazon Relational Database Service (Amazon RDS).

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	rds-instance-default-admin-comprobar	Como los nombres de usuario predeterm inados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de las instancias de bases de datos de Amazon Relational Database Service (Amazon RDS).

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protección de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidencialidad.	redshift-default-admin-check	Como los nombres de usuario predeterminados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de los clústeres de Amazon Redshift.

ID de control	Descripción del control	AWS Config Regla	Directrices
CIP-011-3-R1-Parte 1.2	Cada entidad responsable implementará uno o más programas de protección de la información documentados que incluyan, en conjunto, cada uno de los requisitos aplicables de la tabla R1 de la CIP-011-3 (Protecci ón de la información). Parte 1.2: Métodos para proteger y gestionar de forma segura la BCSI con el fin de mitigar los riesgos de poner en riesgo la confidenc ialidad.	s3- bucket-acl-prohibi ted	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el NERC CIP BCSI.

Prácticas operativas recomendadas para los NCSC Cloud Security Principles

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los principios de seguridad en la nube del Centro Nacional de Ciberseguridad (NCSC) del Reino Unido y las reglas de AWS Config gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de los Principios de Seguridad en la Nube del NCSC del Reino Unido. Un control de los principios de seguridad en la nube de los UK NCSC Cloud Security Principles puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones de controles establecidos en los UK NCSC Cloud Security Principles (National Cyber Security Centre | Cloud security guidance), y dicha información del sector público está licenciada bajo la Open Government Licence v3.0. Puede acceder a la Open Government Licence aquí: Open Government Licence for public sector information.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadam ente protegidos contra la manipulación y el espionaje.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			te Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadamente protegidos contra la manipulación y el espionaje.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadam ente protegidos contra la manipulación y el espionaje.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadam ente protegidos contra la manipulación y el espionaje.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadam ente protegidos contra la manipulación y el espionaje.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadamente protegidos contra la manipulación y el espionaje.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadamente protegidos contra la manipulación y el espionaje.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadam ente protegidos contra la manipulación y el espionaje.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadam ente protegidos contra la manipulación y el espionaje.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadam ente protegidos contra la manipulación y el espionaje.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
1. Protección de datos en tránsito	Los datos de los usuarios que transitan por las redes deben estar adecuadam ente protegidos contra la manipulación y el espionaje.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	api-gw-cache-enabledy cifradas	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	elb-cross-zone-load-habilitado para el balanceo	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	api-gw-cache-enabledy cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2. Protección y resiliencia de los activos	Sus datos (y los activos que los almacenan o procesan) deben estar protegidos adecuadamente.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo dentro de Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configura ción preferida para su organización. En concreto, que tengan períodos de mantenimi ento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVers ionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionar se de forma que impidan, detecten o prevengan los ataques.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5. Seguridad operativa	Los servicios deben operarse y gestionarse de forma que impidan, detecten o prevengan los ataques.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7. Desarrollo seguro	Los servicios en la nube deben diseñarse , desarrollarse e implementarse de manera que se minimicen y mitiguen las amenazas a su seguridad.	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabilitada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7. Desarrollo seguro	Los servicios en la nube deben diseñarse , desarrollarse e implementarse de manera que se minimicen y mitiguen las amenazas a su seguridad.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7. Desarrollo seguro	Los servicios en la nube deben diseñarse , desarrollarse e implementarse de manera que se minimicen y mitiguen las amenazas a su seguridad.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
9. Administración segura de usuarios	Los proveedores deben disponer de herramientas para administrar de forma segura el uso de sus servicios.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autentica das y autorizadas.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizad os para garantiza r que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomenda da de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven compromet idas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autentica das y autorizadas.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autenticadas y autorizadas.	rds-instance-iam-authentication-activado	Asegúrese de que la autenticación AWS Identity and Access Management (IAM) esté habilitada en las instancias del Amazon Relational Database Service (Amazon RDS) para controlar el acceso a los sistemas y activos. De esta manera se fuerza el cifrado del tráfico de red hacia y desde la base de datos mediante la capa de sockets seguros (SSL). No es necesario almacenar credenciales de usuario en la base de datos, ya que la autenticación se administra de forma externa.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autentica das y autorizadas.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autentica das y autorizadas.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autentica das y autorizadas.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autentica das y autorizadas.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autenticadas y autorizadas.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autenticadas y autorizadas.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10. Identidad y autenticación	El acceso a las interfaces de servicio debe restringirse a las personas autenticadas y autorizadas.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo dentro de Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	ecs-container-insights-enabled	La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon Elastic Container Service (ECS) y sus AWS soluciones. Información de contenedores también proporciona información de diagnóstico, como, por ejemplo, errores de reinicio de contenedores, para ayudarlo a aislar problemas y solucionarlos rápidamente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro en la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11. Protección de la interfaz externa	Todas las interfaces externas o de menor confianza del servicio deben identificarse y protegerse.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12. Administración segura del servicio	Los proveedores de servicios en la nube deben reconocer el alto valor de los sistemas de administración.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13. Información de auditoría para los usuarios	Los proveedores deben proporcio nar los registros necesarios para supervisar el acceso a su servicio y los datos que contiene.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13. Información de auditoría para los usuarios	Los proveedores deben proporcio nar los registros necesarios para supervisar el acceso a su servicio y los datos que contiene.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13. Información de auditoría para los usuarios	Los proveedores deben proporcio nar los registros necesarios para supervisar el acceso a su servicio y los datos que contiene.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
13. Información de auditoría para los usuarios	Los proveedores deben proporcio nar los registros necesarios para supervisar el acceso a su servicio y los datos que contiene.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para los principios de seguridad en la nube del NCSC.

Prácticas operativas recomendadas para el NCSC Cyber Assesment Framework

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costos mediante reglas administradas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los controles del Marco de Evaluación Cibernética (CAF) del Centro Nacional de Ciberseguridad (NCSC) del Reino Unido y las reglas de

AWS Config gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles CAF del NCSC del Reino Unido. Un control del UK NCSC CAF puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones de controles establecidos en el UK NCSC CAF (National Cyber Security Centre | NCSC CAF guidance), y dicha información del sector público está licenciada bajo la Open Government Licence v3.0. Puede acceder a la Open Government Licence aquí: Open Government Licence for public sector information.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.a Administración de activos	Se determina y comprende todo lo necesario para entregar, mantener o respaldar las redes y los sistemas de información necesarios para el funcionamiento de las funciones esenciales. Esto incluye los datos, las personas y los sistemas, así como cualquier infraestructura de apoyo (como la alimentación o la refrigeración).	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.
A3.a Administración de activos	Se determina y comprende todo lo necesario para entregar, mantener o respaldar las redes y los sistemas de	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	información necesarios para el funcionamiento de las funciones esenciales. Esto incluye los datos, las personas y los sistemas, así como cualquier infraestructura de apoyo (como la alimentación o la refrigeración).		mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.a Administración de activos	Se determina y comprende todo lo necesario para entregar, mantener o respaldar las redes y los sistemas de información necesarios para el funcionamiento de las funciones esenciales. Esto incluye los datos, las personas y los sistemas, así como cualquier infraestructura de apoyo (como la alimentación o la refrigeración).	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.a Administración de activos	Se determina y comprende todo lo necesario para entregar, mantener o respaldar las redes y los sistemas de información necesarios para el funcionamiento de las funciones esenciales. Esto incluye los datos, las personas y los sistemas, así como cualquier infraestructura de apoyo (como la alimentación o la refrigeración).	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.a Administración de activos	Se determina y comprende todo lo necesario para entregar, mantener o respaldar las redes y los sistemas de información necesarios para el funcionamiento de las funciones esenciales. Esto incluye los datos, las personas y los sistemas, así como cualquier infraestructura de apoyo (como la alimentación o la refrigeración).	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	iam-user-group-membership-compruebe	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosam ente el acceso a las redes y sistemas de información que respaldan la función esencial.	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearch Permite un control de acceso al dominio basado en funciones, así como una seguridad a nivel de índices, documentos y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.a Verificación, autenticación y autorización de identidades	Se verifica, autentica y autoriza rigurosamente el acceso a las redes y sistemas de información que respaldan la función esencial.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.b Administración de dispositivos	Conoce perfectamente los dispositivos que se utilizan para acceder a sus redes, sistemas de información y datos que respaldan su función esencial y confía en ellos.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.b Administración de dispositivos	Conoce perfectamente los dispositivos que se utilizan para acceder a sus redes, sistemas de información y datos que respaldan su función esencial y confía en ellos.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabili tada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	ecs-containers-non privileged	Para ayudar a implementar el principio de privilegio mínimo, las definicio nes de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitad os los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegi os elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	ecs-containers-rea donly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegi o mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegi o mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	efs-access-point-e nforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configura da en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
B2.c Administración de usuarios privilegiados	Se administra estrechamente el acceso de los usuarios privilegiados a las redes y los sistemas de información que respaldan la función esencial.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) puede ayudarlo a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso» : «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	iam-policy-no-stat ements-with-full-a ccess	Asegúrese de que las acciones de IAM se limiten únicament e a las acciones necesarias. Permitir que los usuarios tengan más privilegi os de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	iam-user-group-mem bership-compruebe	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizac iones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	secretsmanager-sec ret-unused	Si existen credencia les no utilizadas en AWS Secrets Manager, debe deshabilitar la opción and/or Eliminar las credenciales, ya que esto podría infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedFor Days (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	guardduty-non-arch ived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasifica ciones para determina r las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.c Administración de usuarios privilegi ados	Se administra estrechamente el acceso de los usuarios privilegi ados a las redes y los sistemas de informaci ón que respaldan la función esencial.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidades y accesos a sus redes y sistemas de información que respaldan la función esencial.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidad es y accesos a sus redes y sistemas de información que respaldan la función esencial.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidades y accesos a sus redes y sistemas de información que respaldan la función esencial.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidades y accesos a sus redes y sistemas de información que respaldan la función esencial.	iam-user-group-membership-compruebe	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidades y accesos a sus redes y sistemas de información que respaldan la función esencial.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidades y accesos a sus redes y sistemas de información que respaldan la función esencial.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidades y accesos a sus redes y sistemas de información que respaldan la función esencial.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidad es y accesos a sus redes y sistemas de información que respaldan la función esencial.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidades y accesos a sus redes y sistemas de información que respaldan la función esencial.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidad es y accesos a sus redes y sistemas de información que respaldan la función esencial.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidades y accesos a sus redes y sistemas de información que respaldan la función esencial.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidades y accesos a sus redes y sistemas de información que respaldan la función esencial.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B2.d Administración de identidades y accesos (IdAM)	Se garantiza una buena administración y mantenimiento del control de identidad es y accesos a sus redes y sistemas de información que respaldan la función esencial.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.a Comprensión de los datos	Se conocen bien los datos importantes para el funcionamiento de la función esencial, dónde se almacenan, dónde se trasladan y cómo la falta de disponibilidad o el acceso, modificación o eliminación no autorizados afectarían negativamente a la función esencial. Esto también se aplica a terceros que almacenen o accedan a datos importantes para la operatividad de funciones esenciales.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	acm-certificate-ex piration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certifica dos deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExp iration (valor de prácticas recomenda das de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	alb-http-drop-invalid-cabecera habilitada	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	vpc-default-security- group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automátic o de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibi lidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexione s o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	elb-cross-zone-loa d-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	elb-deletion-prote ction-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protecció n contra borrado. Utilice esta caracterí stica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibi lidad de sus aplicacio nes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	vpc-vpn-2-tunnels-up	Se pueden implement ar túneles Site-to-S ite VPN redundant es para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectivi dad en caso de que una de las conexione s Site-to-Site VPN no esté disponibl e. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	api-gw-cache-enabl ed-y cifrada	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	opensearch-node-to -node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.b Datos en tránsito	Se ha protegido el tránsito de datos importantes para la operatividad de la función esencial. Esto incluye la transfere ncia de datos a terceros.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que sus AWS CloudTrai l registros estén cifrados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	Habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	sagemaker-endpoint -configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B3.c Datos almacenados	Se han protegido los datos almacenados importantes para la operatividad de la función esencial.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operativi dad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	s3- bucket-default-loc k-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.a Seguridad por diseño	Se ha diseñado la seguridad en la red y los sistemas de información que respaldan la operatividad de las funciones esenciales. Se ha minimizado su superficie expuesta a ataques y se ha asegurado de que la operatividad de la función esencial no se vea afectada por la explotación de una sola vulnerabilidad.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.b Configuración segura	Se han configurado de forma segura la red y los sistemas de información que respaldan la operatividad de las funciones esenciales.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.b Configuración segura	Se han configurado de forma segura la red y los sistemas de información que respaldan la operatividad de las funciones esenciales.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.b Configuración segura	Se han configurado de forma segura la red y los sistemas de información que respaldan la operatividad de las funciones esenciales.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.b Configuración segura	Se han configurado de forma segura la red y los sistemas de información que respaldan la operatividad de las funciones esenciales.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que establezcas el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
B4.c Administración segura	Se administran la red y los sistemas de información de su organización que respaldan la operatividad de las funciones esenciales de modo que se facilite y mantenga la seguridad.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.c Administración segura	Se administran la red y los sistemas de información de su organización que respaldan la operatividad de las funciones esenciale s de modo que se facilite y mantenga la seguridad.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.c Administración segura	Se administran la red y los sistemas de información de su organización que respaldan la operatividad de las funciones esenciale s de modo que se facilite y mantenga la seguridad.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.d. Administración de vulnerabilidades	Se administran las vulnerabilidades conocidas en su red y sus sistemas de información para evitar un impacto adverso en la función esencial.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.d. Administración de vulnerabilidades	Se administran las vulnerabilidades conocidas en su red y sus sistemas de información para evitar un impacto adverso en la función esencial.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.d. Administración de vulnerabilidades	Se administran las vulnerabilidades conocidas en su red y sus sistemas de información para evitar un impacto adverso en la función esencial.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.d. Administración de vulnerabilidades	Se administran las vulnerabilidades conocidas en su red y sus sistemas de información para evitar un impacto adverso en la función esencial.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que establezcas el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
B4.d. Administración de vulnerabilidades	Se administran las vulnerabilidades conocidas en su red y sus sistemas de información para evitar un impacto adverso en la función esencial.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B4.d. Administración de vulnerabilidades	Se administran las vulnerabilidades conocidas en su red y sus sistemas de información para evitar un impacto adverso en la función esencial.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.b Diseño orientado a la resiliencia	Se diseñan la red y los sistemas de información que respaldan su función esencial para ser resilientes ante los incidente s de cibersegu ridad. Los sistemas están debidamen te segregados y se mitigan las limitacio nes de recursos.	elb-cross-zone-loa d-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.b Diseño orientado a la resiliencia	Se diseñan la red y los sistemas de información que respaldan su función esencial para ser resilientes ante los incidente s de cibersegu ridad. Los sistemas están debidamen te segregados y se mitigan las limitacio nes de recursos.	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.b Diseño orientado a la resiliencia	Se diseñan la red y los sistemas de información que respaldan su función esencial para ser resilientes ante los incidente s de cibersegu ridad. Los sistemas están debidamen te segregados y se mitigan las limitacio nes de recursos.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
B5.c Copias de seguridad	Tiene copias de seguridad actualizadas, accesibles y seguras de los datos y la información necesarios para recuperar la operatividad de su función esencial	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta informaci ón para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalm ente los parámetro s de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultane idad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.a Cobertura de monitoreo	Los orígenes de datos que se incluyen en su supervisión permiten identificar oportunamente los eventos de seguridad que podrían afectar la operatividad de su función esencial.	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.b Protección de los registros	Se guardan los datos de registro de forma segura y se concede acceso de lectura solo a las cuentas que sean necesarias para la empresa. Ningún empleado debería tener que modificar o eliminar los datos de registro dentro de un período de retención acordado, tras el cual deberían eliminarse.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identifica de manera confiable y activa las alertas pertinentes.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identifica de manera confiable y activa las alertas pertinentes.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identifica de manera confiable y activa las alertas pertinentes.	s3- event-notifications-enabled	Las notificaciones de eventos de Amazon S3 pueden alertar al personal pertinente de cualquier modificación accidental o intencionada en los objetos de su bucket. Algunos ejemplos de alertas son: creación de un objeto nuevo, eliminación de objetos, restauración de objetos, objetos perdidos o replicados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identific a de manera confiable y activa las alertas pertinentes.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identifica de manera confiable y activa las alertas pertinentes.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identifica de manera confiable y activa las alertas pertinentes.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identific a de manera confiable y activa las alertas pertinentes.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identific a de manera confiable y activa las alertas pertinentes.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identifica de manera confiable y activa las alertas pertinentes.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identific a de manera confiable y activa las alertas pertinentes.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identific a de manera confiable y activa las alertas pertinentes.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identifica de manera confiable y activa las alertas pertinentes.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identific a de manera confiable y activa las alertas pertinentes.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identific a de manera confiable y activa las alertas pertinentes.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identifica de manera confiable y activa las alertas pertinentes.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.c Generación de alertas	La evidencia de posibles incidentes de seguridad contenida en sus datos de monitoreo se identific a de manera confiable y activa las alertas pertinentes.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.d Identificación de incidentes de seguridad	Las alertas se contextualizan con el conocimiento de la amenaza y de sus sistemas para identificar los incidentes de seguridad que requieren algún tipo de respuesta.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.d Identificación de incidentes de seguridad	Las alertas se contextualizan con el conocimiento de la amenaza y de sus sistemas para identificar los incidentes de seguridad que requieren algún tipo de respuesta.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.e Herramientas y capacidades de monitoreo	Las habilidades, herramientas y funciones del personal de monitoreo, incluido el subcontratado, deben ajustarse a los requisitos de gobernanza y presentación de informes, las amenazas esperadas y la complejidad de los datos de red o sistema que necesitan utilizar. El personal de monitoreo conoce las funciones esenciales que debe proteger.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.e Herramientas y capacidades de monitoreo	Las habilidad es, herramientas y funciones del personal de monitoreo , incluido el subcontra tado, deben ajustarse a los requisito s de gobernanz a y presentación de informes, las amenazas esperadas y la complejidad de los datos de red o sistema que necesitan utilizar. El personal de monitoreo conoce las funciones esenciales que debe proteger.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C1.e Herramientas y capacidades de monitoreo	Las habilidad es, herramientas y funciones del personal de monitoreo , incluido el subcontra tado, deben ajustarse a los requisito s de gobernanz a y presentación de informes, las amenazas esperadas y la complejidad de los datos de red o sistema que necesitan utilizar. El personal de monitoreo conoce las funciones esenciales que debe proteger.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C2.a Anomalías del sistema para la detección de ataques	Se definen ejemplos de anomalías en el comportamiento del sistema que proporcionen formas prácticas de detectar actividades maliciosas que, de otro modo, serían difíciles de identificar.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
C2.a Anomalías del sistema para la detección de ataques	Se definen ejemplos de anomalías en el comportamiento del sistema que proporcionen formas prácticas de detectar actividades maliciosas que, de otro modo, serían difíciles de identificar.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
D1.c Pruebas y ejercicios	Su organización lleva a cabo ejercicios para comprobar los planes de respuesta, utilizando incidentes anteriores que afectaron a su organización (y a otras) y escenarios que se basen en la información sobre amenazas y en su evaluación de riesgos.	response-plan-exists-maintained (Verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable. Contar con planes de respuesta actualizados y documentados formalmente puede ayudar a garantizar que el personal de respuesta comprenda los roles, responsabilidades y procesos que deben seguirse durante un incidente.
D1.c Pruebas y ejercicios	Su organización lleva a cabo ejercicios para comprobar los planes de respuesta, utilizando incidentes anteriores que afectaron a su organización (y a otras) y escenarios que se basen en la información sobre amenazas y en su evaluación de riesgos.	response-plan-tested (Verificación del proceso)	Asegúrese de que se prueben los planes de respuesta y recuperación ante incidentes. Esto puede ayudar a comprender si su plan será efectivo durante un incidente y si es necesario abordar alguna laguna o actualización.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el marco de evaluación cibernética del NCSC.

Prácticas operativas recomendadas para redes y servicios de entrega de contenido

Este paquete de conformidad contiene AWS Config reglas basadas en los servicios de redes y entrega de contenido. Para obtener más información, consulte Redes y entrega de contenido en AWS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para los servicios de redes y entrega de contenido.

Prácticas operativas recomendadas para el NIST 800-53 rev 4

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el NIST 800-53 y las reglas de AWS Config administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles NIST 800-53. Un control del NIST 800-53 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

Este paquete de conformidad ha sido validado por AWS Security Assurance Services LLC (AWS SAS), que está formado por un equipo de asesores de seguridad cualificados en el sector de las tarjetas de pago (QSAs), profesionales certificados por HITRUST en el marco de seguridad común (CCSFPs) y profesionales del cumplimiento certificados para ofrecer orientación y evaluaciones en

relación con diversos marcos del sector. AWS Los profesionales de SAS diseñaron este paquete de conformidad para que un cliente pudiera adaptarse a un subconjunto del NIST 800-53.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para

ID de control	Descripción del control	AWS Config Regla	Directrices
			completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y la referencia fundamental de seguridad de las contraseñas de los Centros para la Seguridad de Internet (CIS AWS). Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSymbols (valor de las

ID de control	Descripción del control	AWS Config Regla	Directrices
			mejores prácticas de seguridad AWS funda mentales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(1)	La organización emplea mecanismos automatizados para respaldar la administración de las cuentas del sistema de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(3)	El sistema de información desactiva automáticamente las cuentas inactivas después de [asignación: período de tiempo definido por la organización].	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrail entregará todos los archivos de registro Regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactiva ción y eliminaci ón de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(4)	El sistema de información audita automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas y notifica [asignación: al personal o a los roles definidos por la organización].	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(12)(a)	La organización: a. Monitorea las cuentas del sistema de información para detectar [asignación: un uso atípico definido por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(12)(a)	La organización: a. Monitorea las cuentas del sistema de información para detectar [asignación: un uso atípico definido por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y la referencia fundamental de seguridad de las contraseñas de los Centros para la Seguridad de Internet (CIS) AWS . Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSymbols (valor de las

ID de control	Descripción del control	AWS Config Regla	Directrices
			mejores prácticas de seguridad AWS funda mentales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(f)	La organización: f. Crea, habilita, modifica, deshabilita y elimina las cuentas del sistema de información de acuerdo con [asignación: procedimientos o condiciones definidos por la organización].	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la Cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.
AC-2(g)	La organización: g. Monitorea el uso de las cuentas del sistema de informaci ón.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por el NIST SP 800-63 y la referencia fundament al de seguridad de las contraseñ as de los Centros para la Seguridad de Internet (CIS AWS). Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS funda mentales: verdadero), RequireSy mbols (valor de las

ID de control	Descripción del control	AWS Config Regla	Directrices
			mejores prácticas de seguridad AWS funda mentales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Config Regla	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-2(j)	La organización: j. Revisa las cuentas para comprobar si cumplen con los requisitos de administración de cuentas [asignación: frecuencia definida por la organización].	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-user-group-membership-compruebe	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	s3- -bloques account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Config Regla	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-3	El sistema de información fuerza las autorizaciones aprobadas para el acceso lógico a la información y a los recursos del sistema de acuerdo con las políticas de control de acceso aplicables.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Config Regla	Directrices
			deben asignarse a una VPC.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Config Regla	Directrices
			Amazon VPC para gestionar correctamente el acceso.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	bloques s3 account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas intercone ctados en función de [asignación: políticas de control del flujo de información definidas por la organización].	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-4	El sistema de información fuerza las autorizaciones aprobadas para controlar el flujo de información dentro del sistema y entre sistemas interconectados en función de [asignación: políticas de control del flujo de información definidas por la organización].	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Config Regla	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-5c	La organización: c. Define las autorizaciones de acceso al sistema de información para respaldar la separación de funciones.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- -bloques account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Config Regla	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en sesiones. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6	La organización aplica el principio del privilegio mínimo, que permite únicamente el acceso autorizado a los usuarios (o a los procesos que actúen en nombre de los usuarios) que sean necesarios para llevar a cabo las tareas organizativas asignadas de conformidad con las misiones de la organización y las funciones empresariales.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-6(10)	El sistema de información impide que los usuarios sin privilegios ejecuten funciones con privilegios, como deshabilitar, eludir o alterar las protecciones o contramedidas de seguridad implementadas.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-17(1)	El sistema de información monitorea y controla los métodos de acceso remoto.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
AC-17(2)	El sistema de información implementa mecanismos criptográ ficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-17(2)	El sistema de información implementa mecanismos criptográficos para proteger la confidencialidad y la integridad de las sesiones de acceso remoto.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AC-17(3)	El sistema de información enruta todos los accesos remotos a través de [asignación: número definido por la organización] puntos de control de acceso a la red administrados.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones sobre la información. sharing/collaboration	s3- -bloques account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información sharing/collaboration .	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AC-21(b)	La organización: b. Emplea [Asignación: mecanismos automatizados o procesos manuales definidos por la organización] para ayudar a los usuarios a tomar decisiones relacionadas con la información. sharing/collaboration	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: [asignación: eventos auditables definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuencia de (o situación que requiera) la auditoría de cada evento identificado].	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: [asignaci ón: eventos auditable s definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuenci a de (o situación que requiera) la auditoría de cada evento identificado].	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: [asignación: eventos auditables definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuencia de (o situación que requiera) la auditoría de cada evento identificado].	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la Cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: [asignación: eventos auditables definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuencia de (o situación que requiera) la auditoría de cada evento identificado].	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: [asignaci ón: eventos auditable s definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuenci a de (o situación que requiera) la auditoría de cada evento identificado].	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: [asignación: eventos auditables definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuencia de (o situación que requiera) la auditoría de cada evento identificado].	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará todos los archivos de registro Regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: [asignación: eventos auditables definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuencia de (o situación que requiera) la auditoría de cada evento identificado].	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: [asignaci ón: eventos auditable s definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuenci a de (o situación que requiera) la auditoría de cada evento identificado].	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de informaci ón es capaz de auditar los siguiente s eventos: [asignaci ón: eventos auditable s definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuenci a de (o situación que requiera) la auditoría de cada evento identificado].	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: [asignación: eventos auditables definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuencia de (o situación que requiera) la auditoría de cada evento identificado].	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-2(a)(d)	La organización: a. Determina que el sistema de información es capaz de auditar los siguientes eventos: [asignación: eventos auditables definidos por la organización]; d. Determina que los siguientes eventos deben auditarse dentro del sistema de información: [asignación: eventos auditados definidos por la organización (el subconjunto de los eventos auditables definidos en AU-2 a.) junto con la frecuencia de (o situación que requiera) la auditoría de cada evento identificado].	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la Cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará todos los archivos de registro Regiones de AWS a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-3	El sistema de información genera registros de auditoría que contienen información que establece qué tipo de evento se ha producido, cuándo se ha producido el evento, dónde se ha producido el evento, el origen del evento, el resultado del evento y la identidad de cualquier persona o sujeto relacionados con el evento.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizativos de investigación y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositorios para conocer la situación en toda la organización.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-6(1)(3)	(1) La organización emplea mecanismos automatizados para integrar los procesos de revisión, análisis e informes de auditoría a fin de respaldar los procesos organizat ivos de investiga ción y respuesta a las actividades sospechosas. (3) La organización analiza y correlaciona los registros de auditoría en diferentes repositor ios para conocer la situación en toda la organización.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-7(1)	El sistema de información permite procesar los registros de auditoría de eventos de interés en función de [asignación: campos de auditoría definidos por la organización dentro de los registros de auditoría].	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-7(1)	El sistema de información permite procesar los registros de auditoría de eventos de interés en función de [asignación: campos de auditoría definidos por la organización dentro de los registros de auditoría].	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
AU-9	El sistema de información protege la información de auditoría y las herramientas de auditoría contra todo acceso, modificación y eliminación no autorizados.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.
AU-9	El sistema de información protege la información de auditoría y las herramientas de auditoría contra todo acceso, modificación y eliminación no autorizados.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-9(2)	El sistema de información hace copias de seguridad de los registros de auditoría [asignación: frecuencia definida por la organizac ión] en un sistema o componente del sistema físicamente diferente del sistema o componente que se está auditando.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-11	La organización conserva los registros de auditoría durante [Asignación: período de tiempo definido por la organización de conformidad con la política de retención de registros] a fin de respaldar after-the-fact las investigaciones de incidentes de seguridad y cumplir con los requisitos reglamentarios y organizativos de retención de información.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de información definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de informaci ón definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de informaci ón definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la Cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de informaci ón definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de informaci ón definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de informaci ón definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de informaci ón definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrail entregará todos los archivos de registro Regiones de AWS a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, cuando AWS lance una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de informaci ón definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de informaci ón definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de información definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Config Regla	Directrices
AU-12(a)(c)	El sistema de información: a. Proporciona la capacidad de generar registros de auditoría para los eventos auditables definidos en el AU-2 a. en [asignación: componentes del sistema de informaci ón definidos por la organización]; c. Genera registros de auditoría para los eventos definidos en el AU-2 d. con el contenido definido en el AU-3.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Config Regla	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluació n. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Config Regla	Directrices
CA-7(a)(b)	La organización desarrolla una estrategia de monitoreo continuo e implementa un programa de monitoreo continuo que incluye: a. Establecimiento de las [asignación: métricas definidas por la organización] que se van a monitorea r; b. Establecimiento de las [asignación: frecuencias definidas por la organización] para el monitoreo y las [asignación: frecuencias definidas por la organización] para las evaluaciones que respaldan dicho monitoreo.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorea r la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	ec-2 volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configuración, una configuración de referencia actual del sistema de información.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-2	La organización desarrolla, documenta y mantiene bajo el control de la configura ción, una configura ción de referencia actual del sistema de información.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-7(a)	La organización: a. Configura el sistema de información para proporcionar solo las capacidades esenciales.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-7(a)	La organización: a. Configura el sistema de información para proporcionar solo las capacidades esenciales.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-8(1)	La organización actualiza el inventario de los componentes del sistema de información como parte integral de las instalaciones de componentes, desmontajes y actualizaciones del sistema de información.	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados [asignación: frecuencia definida por la organización] para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados [asignación: frecuencia definida por la organización] para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
CM-8(3)(a)	La organización: a. Emplea mecanismos automatizados [asignación: frecuencia definida por la organización] para detectar la presencia de componentes de hardware, software y firmware no autorizados en el sistema de información	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información en el nivel del sistema contenida en el sistema de informaci ón [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión].	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información en el nivel del sistema contenida en el sistema de información [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperación].	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información en el nivel del sistema contenida en el sistema de informaci ón [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión].	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información en el nivel del sistema contenida en el sistema de informaci ón [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión].	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información en el nivel del sistema contenida en el sistema de informaci ón [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión].	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información en el nivel del sistema contenida en el sistema de informaci ón [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión].	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información en el nivel del sistema contenida en el sistema de informaci ón [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión].	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-9(b)	La organización: b. Realiza copias de seguridad de la información en el nivel del sistema contenida en el sistema de informaci ón [asignación: frecuencia definida por la organización de acuerdo con los objetivos de tiempo y punto de recuperac ión].	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Config Regla	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Config Regla	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de información a un estado conocido tras una interrupción, un peligro o un fallo.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	elb-cross-zone-loa d-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Config Regla	Directrices
CP-10	La organización se encarga de la recuperación y la reconstitución del sistema de informaci ón a un estado conocido tras una interrupción, un peligro o un fallo.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
IA-2	El sistema de información identifica y autentica de forma única a los usuarios de la organización (o los procesos que actúan en nombre de los usuarios de la organización).	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por el NIST SP 800-63 y la referencia fundament al de seguridad de las contraseñ as de los Centros para la Seguridad de Internet (CIS AWS). Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS funda mentales: verdadero), RequireSy mbols (valor de las

ID de control	Descripción del control	AWS Config Regla	Directrices
			mejores prácticas de seguridad AWS funda mentales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
IA-2(1)(11)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (11) El sistema de información implementa la autenticación multifactor para el acceso remoto a cuentas con y sin privilegios, de modo que uno de los factores lo proporciona un dispositivo independiente del sistema al que se accede y el dispositivo cumple [asignación: requisitos de solidez del mecanismo definidos por la organización].	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
IA-2(1)(11)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (11) El sistema de información implementa la autenticación multifactor para el acceso remoto a cuentas con y sin privilegios, de modo que uno de los factores lo proporciona un dispositivo independiente del sistema al que se accede y el dispositivo cumple [asignación: requisitos de solidez del mecanismo definidos por la organización].	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
IA-2(1)(2)(11)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (2) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas sin privilegios. (11) El sistema de información implementa la autenticación multifactor para el acceso remoto a cuentas con y sin privilegios, de modo que uno de los factores lo proporciona un dispositivo independiente del sistema al que se accede y el dispositivo cumple [asignación: requisitos de solidez del mecanismo definidos por la organización].	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Config Regla	Directrices
IA-2(1)(2)(11)	(1) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas con privilegios. (2) El sistema de información implementa la autenticación multifactor para el acceso de red a cuentas sin privilegios. (11) El sistema de información implementa la autenticación multifactor para el acceso remoto a cuentas con y sin privilegios, de modo que uno de los factores lo proporciona un dispositivo independiente del sistema al que se accede y el dispositivo cumple [asignación: requisitos de solidez del mecanismo definidos por la organización].	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Config Regla	Directrices
IA-5(1)(a)(d)(e)	Para la autenticación basada en contraseñas, el sistema de información: a. Aplica una complejidad mínima de las contraseñas con [asignación: requisitos definidos por la organización en cuanto a la distinción entre mayúsculas y minúsculas, números de caracteres, mezcla de letras mayúsculas y letras minúsculas, números y caracteres especiales, incluidos los requisitos mínimos de cada tipo]; d. Aplica las restricciones de duración mínima y máxima de las contraseñas de [asignación: números definidos por la organización para una vida útil mínima y máxima]; e. Prohíbe la reutilización de contraseñas durante [asignación: número definido	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y la referencia fundamental de seguridad de las contraseñas de los Centros para la Seguridad de Internet (CIS AWS). Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSymbols (valor de las

ID de control	Descripción del control	AWS Config Regla	Directrices
	por la organización] generaciones.		mejores prácticas de seguridad AWS funda mentales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
IA-5(4)	La organización emplea herramientas automatizadas para determinar si los autenticadores de contraseñas son lo suficientemente seguros como para cumplir [asignación: los requisitos definidos por la organización].	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por el NIST SP 800-63 y la referencia de seguridad de las contraseñas de la AWS Fundación Centers for Internet Security (CIS). Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSymbols (valor de las

ID de control	Descripción del control	AWS Config Regla	Directrices
			mejores prácticas de seguridad AWS funda mentales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
IA-5(7)	La organización se asegura de que los autenticadores estáticos no cifrados no estén integrados en las aplicaciones o los scripts de acceso ni se almacenen en las teclas de función.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Config Regla	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
IR-4(1)	La organización emplea mecanismos automatizados para respaldar el proceso de gestión de incidentes.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
IR-6(1)	La organización emplea mecanismos automatizados para ayudar a denunciar los incidentes de seguridad.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
IR-7(1)	La organización emplea mecanismos automatizados para aumentar la disponibilidad de la información y el apoyo relacionados con la respuesta a los incidentes.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
RA-5	La organización: a. Busca vulnerabilidades en el sistema de información y en las aplicaciones alojadas [Asignación: frecuencia definida por la organización de and/or forma aleatoria de acuerdo con el proceso definido por la organización] y cuando se identifican y notifican nuevas vulnerabilidades que puedan afectar al sistema o a las aplicaciones; b. Emplea herramientas y técnicas de análisis de vulnerabilidades que facilitan la interoperabilidad entre las herramientas y automatizan partes del proceso de administración de vulnerabilidades mediante el uso de estándares para: 1. Enumerar las plataformas, los defectos del software	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
	y las configura ciones incorrectas; 2. Formatear las listas de verificac ión y los procedimi entos de prueba; y 3. Medir el impacto de la vulnerabi lidad; c. Analiza los informes de análisis de vulnerabilidades y los resultados de las evaluacio nes de control de seguridad; d. Corrige las vulnerabilidades legítimas [asignación: tiempos de respuesta definidos por la organización], de acuerdo con una evaluación organizat iva del riesgo; y e. Comparte la informaci ón obtenida del proceso de análisis de vulnerabilidades y las evaluaciones de control de seguridad con [asignación: personal o roles definidos por la organización] para ayudar a eliminar		

ID de control	Descripción del control	AWS Config Regla	Directrices
	vulnerabilidades similares en otros sistemas de informaci ón (es decir, debilidad es o deficiencias sistémicas).		

ID de control	Descripción del control	AWS Config Regla	Directrices
RA-5	La organización: a. Realiza análisis en busca de vulnerabilidades en el sistema de información y en las aplicaciones alojadas [Asignación: frecuencia definida por la organización de and/or forma aleatoria de acuerdo con el proceso definido por la organización] y cuando se identifican y notifican nuevas vulnerabilidades que puedan afectar al sistema o a las aplicaciones; b. Emplea herramientas y técnicas de análisis de vulnerabilidades que facilitan la interoperabilidad entre las herramientas y automatizan partes del proceso de administración de vulnerabilidades mediante el uso de estándares para: 1. Enumerar las plataformas, los	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
	defectos del software y las configura ciones incorrectas; 2. Formatear las listas de verificac ión y los procedimi entos de prueba; y 3. Medir el impacto de la vulnerabi lidad; c. Analiza los informes de análisis de vulnerabilidades y los resultados de las evaluacio nes de control de seguridad; d. Corrige las vulnerabilidades legítimas [asignación: tiempos de respuesta definidos por la organización], de acuerdo con una evaluación organizat iva del riesgo; y e. Comparte la informaci ón obtenida del proceso de análisis de vulnerabilidades y las evaluaciones de control de seguridad con [asignación: personal o roles definidos por la organización] para		

ID de control	Descripción del control	AWS Config Regla	Directrices
	ayudar a eliminar vulnerabilidades similares en otros sistemas de información (es decir, debilidades o deficiencias sistémicas).		
SA-3(a)	La organización: a. Administra el sistema de información mediante [asignación: el ciclo de vida de desarrollo del sistema definido por la organización] que incorpora consideraciones de seguridad de la información.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Config Regla	Directrices
SA-3(a)	La organización: a. Administra el sistema de información mediante [asignación: el ciclo de vida de desarrollo del sistema definido por la organización] que incorpora consideraciones de seguridad de la información.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
SA-3(a)	La organización: a. Administra el sistema de información mediante [asignación: el ciclo de vida de desarrollo del sistema definido por la organización] que incorpora consideraciones de seguridad de la información.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Config Regla	Directrices
SA-10	La organización exige al desarrollador del sistema de informaci ón, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el [selección (ona o varias opciones): el diseño, el desarrollo, la implementación y el funcionamiento] del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
	Documente los cambios aprobados en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	AWS Config Regla	Directrices
SA-10	La organización exige al desarrollador del sistema de información, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el [selección (ona o varias opciones): el diseño, el desarrollo, la implementación y el funcionamiento] del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
	Documente los cambios aprobados en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	AWS Config Regla	Directrices
SA-10	La organización exige al desarrollador del sistema de informaci ón, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el [selección (ona o varias opciones): el diseño, el desarrollo, la implementación y el funcionamiento] del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
	Documente los cambios aprobados en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	AWS Config Regla	Directrices
SA-10	La organización exige al desarrollador del sistema de informaci ón, del component e del sistema o del servicio del sistema de información que: a. Gestione la configuración durante el [selección (ona o varias opciones): el diseño, el desarrollo, la implementación y el funcionamiento] del sistema, component e o servicio; b. Documente, administr e y controle la integridad de los cambios en [asignaci ón: elementos de la configuración definidos por la organización en el marco de la gestión de la configura ción]; c. Implement e únicament e los cambios aprobados por la organización en el sistema, component e o servicio; d.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
	Documente los cambios aprobados en el sistema, componente o servicio y los posibles impactos de dichos cambios en la seguridad; y e. Realice un seguimiento de los defectos de seguridad y de su resolución en el sistema, componente o servicio y notifique los resultados [asignación: al personal definido por la organización].		

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de informaci ón.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-2	El sistema de información separa la funcionalidad del usuario (incluidos los servicios de la interfaz de usuario) de la funcionalidad de administración del sistema de información.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-4	El sistema de información impide la transferencia de información no autorizada e involuntaria a través de los recursos compartidos del sistema.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Config Regla	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Config Regla	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignaci ón: tipos de ataques de denegación de servicio definidos por la organizac ión o referencias a las fuentes de dicha información] mediante la aplicació n de [asignación: medidas de seguridad definidas por la organización].	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-5	El sistema de información protege o limita los efectos de los siguientes tipos de ataques de denegación de servicio: [asignación: tipos de ataques de denegación de servicio definidos por la organización o referencias a las fuentes de dicha información] mediante la aplicación de [asignación: medidas de seguridad definidas por la organización].	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Config Regla	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Config Regla	Directrices
			deben asignarse a una VPC.
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibi lidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	s3- -bloquea account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los componentes del sistema de acceso público que están [selección: física o lógicamente] separados de las redes organizativas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interfaces administradas que constan de dispositivos de protección perimetral dispuestos de acuerdo con una arquitectura de seguridad organizativa.	alb-http-drop-invalid-habilitado para encabezados	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7	El sistema de información: a. Monitorea y controla las comunicaciones en el límite externo del sistema y en los límites internos clave dentro del sistema; b. Implementa subredes para los component es del sistema de acceso público que están [selección: física o lógicamen te] separados de las redes organizat ivas internas; y c. Se conecta a redes o sistemas de información externos únicamente a través de interface s administradas que constan de dispositi vos de protección perimetral dispuesto s de acuerdo con una arquitectura de seguridad organizat iva.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Config Regla	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Config Regla	Directrices
			deben asignarse a una VPC.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	bloques s3 account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-7(3)	La organización limita el número de conexiones de red externas al sistema de información.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de la información transmitida.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de la información transmitida.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de la información transmitida.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de la información transmitida.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8	El sistema de información protege la [selección (una o varias): confidenc ialidad, integridad] de la información transmitida.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8	El sistema de información protege la [selección (una o varias): confidenc ialidad, integridad] de la información transmitida.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de la información transmitida.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-8(1)	El sistema de información implementa mecanismos criptográficos para [seleccionar (una o más): impedir la divulgación no autorizada de información; detectar cambios en la información] durante la transmisión, a menos que esté protegida de otra manera con [asignación: protecciones físicas alternativas definidas por la organización].	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-12	La organización establece y administra las claves criptográficas para la criptografía requerida empleada en el sistema de información de acuerdo con [asignación: requisitos definidos por la organización para la generación, distribución, almacenamiento, acceso y destrucción de claves].	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-12	La organización establece y administra las claves criptográficas para la criptografía requerida empleada en el sistema de información de acuerdo con [asignación: requisitos definidos por la organización para la generación, distribución, almacenamiento, acceso y destrucción de claves].	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-12	La organización establece y administra las claves criptográficas para la criptografía requerida empleada en el sistema de información de acuerdo con [asignación: requisitos definidos por la organización para la generación, distribución, almacenamiento, acceso y destrucción de claves].	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	Habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa [asignación: usos criptográficos definidos por la organización y tipo de criptografía requerida para cada uso] de conformidad con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-13	El sistema de información implementa criptografía validada por las FIPS o aprobada por la NSA de conformidad con leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y estándares aplicables.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-23	El sistema de información protege la autenticidad de las sesiones de comunicación.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	api-gw-cache-enabled-y cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-28	El sistema de información protege la [selección (una o varias): confidencialidad, integridad] de [asignación: información en reposo definida por la organización].	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-36	La organización distribuye [asignación: procesamiento y almacenamiento definidos por la organización] en varias ubicaciones físicas.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Config Regla	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Config Regla	Directrices
SC-36	La organización distribuye [asignación: procesamiento y almacenamiento definidos por la organización] en varias ubicaciones físicas.	rds-cluster-multi-az-habilitado	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Config Regla	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
SC-36	La organización distribuye [asignaci ón: procesamiento y almacenamiento definidos por la organización] en varias ubicaciones físicas.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-2(2)	La organización emplea mecanismos automatizados [asignación: frecuencia definida por la organización] para determinar el estado de los componentes del sistema de información con respecto a la corrección de fallos.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-2(2)	La organización emplea mecanismos automatizados [asignación: frecuencia definida por la organización] para determinar el estado de los componentes del sistema de información con respecto a la corrección de fallos.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-2(2)	La organización emplea mecanismos automatizados [asignación: frecuencia definida por la organización] para determinar el estado de los componentes del sistema de información con respecto a la corrección de fallos.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(1)	La organización conecta y configura las herramientas individuales de detección de intrusos en un sistema de detección de intrusos que abarca todo el sistema de informaci ón.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
SI-4(2)	La organización emplea herramientas automatizadas para respaldar el análisis de los eventos casi en tiempo real.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente [asignación: frecuencia definida por la organización] para detectar actividades o condiciones inusuales o no autorizadas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente [asignación: frecuencia definida por la organización] para detectar actividades o condiciones inusuales o no autorizadas.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente [asignación: frecuencia definida por la organización] para detectar actividades o condiciones inusuales o no autorizadas.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(4)	El sistema de información monitorea el tráfico de comunicaciones entrante y saliente [asignación: frecuencia definida por la organización] para detectar actividades o condiciones inusuales o no autorizadas.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(5)	El sistema de información alerta [asignación: al personal o los roles definidos por la organización] cuando se presentan los siguientes indicios de riesgo o posible riesgo: [asignación: indicadores de riesgo definidos por la organización].	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(16)	La organización correlaciona la información de las herramientas de monitoreo empleadas en todo el sistema de información.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Config Regla	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Config Regla	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Config Regla	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Config Regla	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Config Regla	Directrices
	de transacciones de interés para la organización.		

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-4(a)(b)(c)	La organización: a. Monitorea el sistema de información para detectar: 1. Ataques e indicadores de posibles ataques de acuerdo con [asignación: objetivos de monitoreo definidos por la organización]; y 2. Conexiones locales, de red y remotas no autorizadas; b. Identifica el uso no autorizado del sistema de información mediante [asignación: técnicas y métodos definidos por la organización]; c. Implementa dispositivos de monitoreo: i. estratégicamente dentro del sistema de información para recopilar información esencial determinada por la organización; y (ii) en ubicaciones ad hoc específicas del sistema para rastrear tipos específicos	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Config Regla	Directrices
	de transacciones de interés para la organización.		
SI-7	La organización emplea herramientas de verificación de la integridad para detectar cambios no autorizados en [asignación: software, firmware e información definidos por la organización].	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-7(1)	El sistema de información realiza una comprobación de la integridad de [asignación: software, firmware e información definidos por la organización] [selección (una o más): al inicio; en [asignación: estados transitorios definidos por la organización o eventos relevantes para la seguridad]; [asignación: frecuencia definida por la organización]].	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-7(1)	El sistema de información realiza una comprobación de la integridad de [asignación: software, firmware e información definidos por la organización] [selección (una o más): al inicio; en [asignación: estados transitorios definidos por la organización o eventos relevantes para la seguridad]; [asignación: frecuencia definida por la organización]].	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-7(1)	El sistema de información realiza una comprobac ión de la integrida d de [asignación: software, firmware e información definidos por la organización] [selección (una o más): al inicio; en [asignación: estados transitorios definidos por la organización o eventos relevante s para la seguridad]; [asignación: frecuenci a definida por la organización]].	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Config Regla	Directrices
SI-12	La organización administra y conserva la información del sistema de información y aquella producida por el sistema de conformidad con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas, directrices y requisitos operativos aplicables.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el NIST 800-53 rev. 4.

Prácticas operativas recomendadas para el NIST 800-53 rev 5

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el NIST 800-53 y las reglas de AWS Config administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno

o más controles NIST 800-53. Un control del NIST 800-53 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	Administración de cuentas | Acciones de auditoría automatiz adas	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.
AC-2(4)	Administración de cuentas | Acciones de auditoría automatiz adas	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	Administración de cuentas | Acciones de auditoría automatizadas	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
AC-2(4)	Administración de cuentas | Acciones de auditoría automatizadas	cloud-trail-cloud-watch-habilitados para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	Administración de cuentas | Acciones de auditoría automatizadas	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	Administración de cuentas | Acciones de auditoría automatiz adas	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
AC-2(4)	Administración de cuentas | Acciones de auditoría automatiz adas	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	Administración de cuentas | Acciones de auditoría automatizadas	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(4)	Administración de cuentas | Acciones de auditoría automatiz adas	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2(12)	Administración de cuentas | Supervisión de cuentas para usos atípicos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	Administración de cuentas	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	Administración de cuentas	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	Administración de cuentas	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	Administración de cuentas	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC-2	Administración de cuentas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	Administración de cuentas	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-2	Administración de cuentas	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecio nal y obligatorio	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecio nal y obligatorio	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecio nal y obligatorio	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecio nal y obligatorio	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecio nal y obligatorio	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecio nal y obligatorio	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3(15)	Aplicación de normas de acceso | Control de acceso discrecional y obligatorio	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.
AC-3	Aplicación de normas de acceso	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implement ar controles para restringir los cambios en los metadatos de la instancia.
AC-3	Aplicación de normas de acceso	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
AC-3	Aplicación de normas de acceso	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-3	Aplicación de normas de acceso	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC-3	Aplicación de normas de acceso	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC-3	Aplicación de normas de acceso	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC-3	Aplicación de normas de acceso	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
AC-3	Aplicación de normas de acceso	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-3	Aplicación de normas de acceso	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-3	Aplicación de normas de acceso	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-4(26)	Control del flujo de información | Acciones de filtrado de auditorías	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5	Separación de funciones	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5	Separación de funciones	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.
AC-5	Separación de funciones	iam-policy-no-stat ements-with-full-a ccess	Asegúrese de que las acciones de IAM se limiten únicament e a las acciones necesarias. Permitir que los usuarios tengan más privilegi os de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5	Separación de funciones	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-5	Separación de funciones	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC-5	Separación de funciones	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(2)	Privilegio mínimo | Acceso sin privilegios para funciones no relacionadas con la seguridad	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(2)	Privilegio mínimo | Acceso sin privilegios para funciones no relacionadas con la seguridad	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(2)	Privilegio mínimo | Acceso sin privilegios para funciones no relacionadas con la seguridad	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(3)	Privilegio mínimo | Acceso de red a comandos con privilegios	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(3)	Privilegio mínimo | Acceso de red a comandos con privilegios	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(3)	Privilegio mínimo | Acceso de red a comandos con privilegios	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(3)	Privilegio mínimo | Acceso de red a comandos con privilegios	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
AC-6(3)	Privilegio mínimo | Acceso de red a comandos con privilegios	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(3)	Privilegio mínimo | Acceso de red a comandos con privilegios	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(9)	Privilegio mínimo | Registro del uso de las funciones con privilegios	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(9)	Privilegio mínimo | Registro del uso de las funciones con privilegios	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(9)	Privilegio mínimo | Registro del uso de las funciones con privilegios	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
AC-6(9)	Privilegio mínimo | Registro del uso de las funciones con privilegios	cloud-trail-cloud-watch-habilitados para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(9)	Privilegio mínimo | Registro del uso de las funciones con privilegios	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(9)	Privilegio mínimo | Registro del uso de las funciones con privilegios	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
AC-6(9)	Privilegio mínimo | Registro del uso de las funciones con privilegios	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(9)	Privilegio mínimo | Registro del uso de las funciones con privilegios	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(9)	Privilegio mínimo | Registro del uso de las funciones con privilegios	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(10)	Privilegio mínimo | Prohibición de ejecutar funciones con privilegios a los usuarios sin privilegios	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(10)	Privilegio mínimo | Prohibición de ejecutar funciones con privilegios a los usuarios sin privilegios	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-6(10)	Privilegio mínimo | Prohibición de ejecutar funciones con privilegios a los usuarios sin privilegios	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(2)	Acceso remoto | Protección de la confidencialidad y la integridad mediante el cifrado	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
AC-17(2)	Acceso remoto | Protección de la confidencialidad y la integridad mediante el cifrado	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(2)	Acceso remoto | Protección de la confidencialidad y la integridad mediante el cifrado	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
AC-17(2)	Acceso remoto | Protección de la confidencialidad y la integridad mediante el cifrado	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(2)	Acceso remoto | Protección de la confidencialidad y la integridad mediante el cifrado	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
AC-17(2)	Acceso remoto | Protección de la confidencialidad y la integridad mediante el cifrado	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-17(2)	Acceso remoto | Protección de la confidencialidad y la integridad mediante el cifrado	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
AC-21	Intercambio de información	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
AC-21	Intercambio de información	ssm-document-not-p ublic	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.
AC-21	Intercambio de información	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
AC-21	Intercambio de información	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
AC-21	Intercambio de información	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
AC-21	Intercambio de información	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
AC-21	Intercambio de información	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
AC-21	Intercambio de información	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
AC-21	Intercambio de información	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AC-21	Intercambio de información	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-2	Registro de eventos	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-2	Registro de eventos	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-3	Contenido de los registros de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-3	Contenido de los registros de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
AU-6(1)	Revisión, análisis e informes de registros de auditoría | Integraci ón de procesos automatizados	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)	Revisión, análisis e informes de registros de auditoría | Integración de procesos automatizados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)	Revisión, análisis e informes de registros de auditoría | Integración de procesos automatizados	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(1)	Revisión, análisis e informes de registros de auditoría | Integración de procesos automatizados	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(3)	Revisión, análisis e informes de registros de auditoría | Correlación de repositorios de registro de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(4)	Revisión, análisis e informes de registros de auditoría | Revisión y análisis centrales	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
AU-6(5)	Revisión, análisis e informes de registros de auditoría | Análisis integrado de registros de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(5)	Revisión, análisis e informes de registros de auditoría | Análisis integrado de registros de auditoría	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(5)	Revisión, análisis e informes de registros de auditoría | Análisis integrado de registros de auditoría	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-6(5)	Revisión, análisis e informes de registros de auditoría | Análisis integrado de registros de auditoría	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-7(1)	Reducción de registros de auditoría y generación de informes | Procesamiento automático	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
AU-9(2)	Protección de la información de auditoría | Almacenamiento en sistemas o componentes físicos separados	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9(2)	Protección de la información de auditoría | Almacenamiento en sistemas o componentes físicos separados	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9(2)	Protección de la información de auditoría | Almacenamiento en sistemas o componentes físicos separados	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9(7)	Protección de la información de auditoría | Almacenamiento en un componente con un sistema operativo diferente	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
AU-9	Protección de la información de auditoría	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9	Protección de la información de auditoría	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
AU-9	Protección de la información de auditoría	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenc iales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9	Protección de la información de auditoría	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-9	Protección de la información de auditoría	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-10	No repudio	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-10	No repudio	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
AU-12	Generación de registros de auditoría	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-12	Generación de registros de auditoría	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
AU-14(1)	Auditoría de sesión | Puesta en marcha del sistema	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
CA-7	Monitoreo continuo	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspondiente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
CA-7	Monitoreo continuo	s3- event-notifications-enabled	Las notificaciones de eventos de Amazon S3 pueden alertar al personal pertinente de cualquier modificación accidental o intencionada en los objetos de su bucket. Algunos ejemplos de alertas son: creación de un objeto nuevo, eliminación de objetos, restauración de objetos, objetos perdidos o replicados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
CA-7	Monitoreo continuo	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CA-7	Monitoreo continuo	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-7	Monitoreo continuo	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales almacenados, asegúrese de que sus AWS CodeBuild artefactos estén cifrados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	rds-instance-default-admin-comprobar	Como los nombres de usuario predeterminados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de las instancias de bases de datos de Amazon Relational Database Service (Amazon RDS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	api-gw-cache-enabled-y cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	efs-encrypted-check	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	redshift-default-admin-check	Como los nombres de usuario predeterminados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de los clústeres de Amazon Redshift.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	sagemaker-endpoint -configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CA-9(1)	Conexiones internas del sistema | Comprobaciones de conformidad	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2(2)	Configuración de referencia | Compatibilidad con la automatización para la precisión y la vigencia	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2(2)	Configuración de referencia | Compatibilidad con la automatización para la precisión y la vigencia	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2(2)	Configuración de referencia | Compatibilidad con la automatización para la precisión y la vigencia	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2(2)	Configuración de referencia | Compatibilidad con la automatización para la precisión y la vigencia	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2(2)	Configuración de referencia | Compatibilidad con la automatización para la precisión y la vigencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2(2)	Configuración de referencia | Compatibilidad con la automatización para la precisión y la vigencia	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	Configuración de referencia	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
CM-2	Configuración de referencia	rds-instance-default-admin-comprobar	Como los nombres de usuario predeterminados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de las instancias de bases de datos de Amazon Relational Database Service (Amazon RDS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	Configuración de referencia	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	Configuración de referencia	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	Configuración de referencia	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	Configuración de referencia	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	Configuración de referencia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	Configuración de referencia	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	Configuración de referencia	redshift-default-admin-check	Como los nombres de usuario predeterminados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de los clústeres de Amazon Redshift.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-2	Configuración de referencia	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	api-gw-cache-enabled-y cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3(6)	Control de cambios de configuración | Administración de la criptografía	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-3	Control de cambios de la configuración	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
CM-3	Control de cambios de la configuración	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-7	Funcionalidad mínima	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
CM-7	Funcionalidad mínima	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-7	Funcionalidad mínima	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(1)	Inventario de componentes del sistema | Actualizaciones durante la instalación y la retirada	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(1)	Inventario de componentes del sistema | Actualizaciones durante la instalación y la retirada	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(2)	Inventario de componentes del sistema | Mantenimiento automatizado	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(3)	Inventario de componentes del sistema | Detección automática de componentes no autorizados	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(3)	Inventario de componentes del sistema | Detección automática de componentes no autorizados	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(3)	Inventario de componentes del sistema | Detección automática de componentes no autorizados	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8(3)	Inventario de componentes del sistema | Detección automática de componentes no autorizados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8	Inventario de componentes del sistema	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CM-8	Inventario de componentes del sistema	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-2(2)	Plan de contingencia | Planificación de la capacidad	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-2(2)	Plan de contingencia | Planificación de la capacidad	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(1)	Sitio de almacenamiento alternativo | Separación del sitio principal	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(1)	Sitio de almacenamiento alternativo | Separación del sitio principal	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(1)	Sitio de almacenamiento alternativo | Separación del sitio principal	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(1)	Sitio de almacenamiento alternativo | Separación del sitio principal	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(1)	Sitio de almacenamiento alternativo | Separación del sitio principal	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(1)	Sitio de almacenamiento alternativo | Separación del sitio principal	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(1)	Sitio de almacenamiento alternativo | Separación del sitio principal	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(1)	Sitio de almacenamiento alternativo | Separación del sitio principal	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	elasticache-redis-cluster-automatic-comprobación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
CP-6(2)	Sitio de almacenam iento alternativo | Objetivos de tiempos y puntos de recuperac ión	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6(2)	Sitio de almacenamiento alternativo | Objetivos de tiempos y puntos de recuperación	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6	Sitio de almacenamiento alternativo	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6	Sitio de almacenamiento alternativo	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6	Sitio de almacenamiento alternativo	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6	Sitio de almacenamiento alternativo	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6	Sitio de almacenamiento alternativo	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6	Sitio de almacenamiento alternativo	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6	Sitio de almacenamiento alternativo	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-6	Sitio de almacenamiento alternativo	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-9	Backup del sistema	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
CP-10	Recuperación y reconstitución del sistema	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CP-10	Recuperación y reconstitución del sistema	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)	Identificación y autenticación (usuarios de la organización) | Autenticación multifactor en cuentas con privilegios	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)	Identificación y autenticación (usuarios de la organización) | Autenticación multifactor en cuentas con privilegios	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)	Identificación y autenticación (usuarios de la organización) | Autenticación multifactor en cuentas con privilegios	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(1)	Identificación y autenticación (usuarios de la organización) | Autenticación multifactor en cuentas con privilegios	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(2)	Identificación y autenticación (usuarios de la organización) | Autenticación multifactor en cuentas sin privilegios	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(2)	Identificación y autenticación (usuarios de la organización) | Autenticación multifactor en cuentas sin privilegios	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(2)	Identificación y autenticación (usuarios de la organización) | Autenticación multifactor en cuentas sin privilegios	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(2)	Identificación y autenticación (usuarios de la organización) | Autenticación multifactor en cuentas sin privilegios	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(6)	Identificación y autenticación (usuarios de la organización) | Acceso a las cuentas - Dispositivo independiente	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(6)	Identificación y autenticación (usuarios de la organización) | Acceso a las cuentas - Dispositivo independiente	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(6)	Identificación y autenticación (usuarios de la organización) | Acceso a las cuentas - Dispositivo independiente	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(6)	Identificación y autenticación (usuarios de la organización) | Acceso a las cuentas - Dispositivo independiente	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(8)	Identificación y autenticación (usuarios de la organización) | Acceso a las cuentas - Resistente a la reproducción	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(8)	Identificación y autenticación (usuarios de la organización) | Acceso a las cuentas - Resistente a la reproducción	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(8)	Identificación y autenticación (usuarios de la organización) | Acceso a las cuentas - Resistente a la reproducción	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-2(8)	Identificación y autenticación (usuarios de la organización) | Acceso a las cuentas - Resistente a la reproducción	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
IA-5(1)	Administración de autenticadores | Autenticación basada en contraseñas	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5(1)	Administración de autenticadores | Autenticación basada en contraseñas	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
IA-5(1)	Administración de autenticadores | Autenticación basada en contraseñas	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5(1)	Administración de autenticadores | Autenticación basada en contraseñas	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
IA-5(1)	Administración de autenticadores | Autenticación basada en contraseñas	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5(1)	Administración de autenticadores | Autenticación basada en contraseñas	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5(1)	Administración de autenticadores | Autenticación basada en contraseñas	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5(1)	Administración de autenticadores | Autenticación basada en contraseñas	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IA-5(7)	Administración de autenticadores | Sin autenticadores estáticos no cifrados integrados	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4(1)	Gestión de incidentes | Procesos automatizados de gestión de incidentes	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
IR-4(5)	Gestión de incidentes | Desactivación automática del sistema	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RA-3(4)	Evaluación de riesgos | Ciberanálisis predictivo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-3	Ciclo de vida de desarrollo del sistema	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-3	Ciclo de vida de desarrollo del sistema	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-8(19)	Principios de ingeniería de seguridad y privacidad | Protección continua	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-8(21)	Principios de ingeniería de seguridad y privacidad | Autoanálisis	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-8(22)	Principios de ingeniería de seguridad y privacidad | Responsabilidad y trazabilidad	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-8(25)	Principios de ingeniería de seguridad y privacidad | Seguridad económica	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-11(1)	Pruebas y evaluación para desarrolladores | Análisis de código estático	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-11(6)	Pruebas y evaluación para desarrolladores | Revisiones de superficies expuestas a ataques	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-15(2)	Proceso de desarrollo, estándares y herramientas | Herramientas de seguimiento de seguridad y privacidad	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-15(2)	Proceso de desarrollo, estándares y herramientas | Herramientas de seguimiento de seguridad y privacidad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-15(8)	Proceso de desarrollo, estándares y herramientas | Reutilización de información sobre amenazas y vulnerabilidades	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SA-15(8)	Proceso de desarrollo, estándares y herramientas | Reutilización de información sobre amenazas y vulnerabilidades	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(1)	Denial-of-service Protección | Restrinja la capacidad de atacar otros sistemas	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(2)	Denial-of-service Protección | Capacidad, ancho de banda y redundancia	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5(3)	Denial-of-service Protección | Detección y monitoreo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-5	Denial-of-service Protección	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
SC-7(3)	Protección perimetral | Puntos de acceso	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.
SC-7(3)	Protección perimetral | Puntos de acceso	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
SC-7(3)	Protección perimetral | Puntos de acceso	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(3)	Protección perimetral | Puntos de acceso	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7(3)	Protección perimetral | Puntos de acceso	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SC-7(3)	Protección perimetral | Puntos de acceso	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SC-7(3)	Protección perimetral | Puntos de acceso	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-7(3)	Protección perimetral | Puntos de acceso	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(3)	Protección perimetral | Puntos de acceso	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(4)	Protección perimetral | Servicios de telecomunicaciones externos	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(5)	Protección perimetral | Denegar de forma predeterminada - permitir de forma excepcional	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(5)	Protección perimetral | Denegar de forma predeterminada - permitir de forma excepcional	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(5)	Protección perimetral | Denegar de forma predeterminada - permitir de forma excepcional	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(5)	Protección perimetral | Denegar de forma predeterminada - permitir de forma excepcional	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(9)	Protección perimetral | Restricción del tráfico amenazante de comunicaciones salientes	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.
SC-7(10)	Protección perimetral | Prevención de la exfiltración	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
SC-7(10)	Protección perimetral | Prevención de la exfiltración	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
SC-7(10)	Protección perimetral | Prevención de la exfiltración	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SC-7(10)	Protección perimetral | Prevención de la exfiltración	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
SC-7(10)	Protección perimetral | Prevención de la exfiltración	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	Habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
SC-7(10)	Protección perimetral | Prevención de la exfiltración	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(10)	Protección perimetral | Prevención de la exfiltración	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
SC-7(10)	Protección perimetral | Prevención de la exfiltración	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(11)	Protección perimetral | Restricción del tráfico de comunicaciones entrantes	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(16)	Protección perimetral | Prevención de la detección de componentes del sistema	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7(21)	Protección perimetral | Aislamiento de los componentes del sistema	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
SC-7	Protección perimetral	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
SC-7	Protección perimetral	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
SC-7	Protección perimetral	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
SC-7	Protección perimetral	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
SC-7	Protección perimetral	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
SC-7	Protección perimetral	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
SC-7	Protección perimetral	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
SC-7	Protección perimetral	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-7	Protección perimetral	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(1)	Confidencialidad e integridad de la transmisión | Protección criptográfica	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8(2)	Confidencialidad e integridad de la transmisión | Gestión previa y posterior a la transmisión	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	Confidencialidad e integridad de la transmisión	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	Confidencialidad e integridad de la transmisión	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-8	Confidencialidad e integridad de la transmisión	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	Confidencialidad e integridad de la transmisión	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
SC-8	Confidencialidad e integridad de la transmisión	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	Confidencialidad e integridad de la transmisión	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-8	Confidencialidad e integridad de la transmisión	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	Confidencialidad e integridad de la transmisión	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-8	Confidencialidad e integridad de la transmisión	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-8	Confidencialidad e integridad de la transmisión	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-12(2)	Establecimiento y administración de claves criptográficas | Claves simétricas	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12(2)	Establecimiento y administración de claves criptográficas | Claves simétricas	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12(3)	Establecimiento y administración de claves criptográficas | Claves asimétricas	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-12(3)	Establecimiento y administración de claves criptográficas | Claves asimétricas	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12(3)	Establecimiento y administración de claves criptográficas | Claves asimétricas	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
SC-12(3)	Establecimiento y administración de claves criptográficas | Claves asimétricas	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12(3)	Establecimiento y administración de claves criptográficas | Claves asimétricas	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
SC-12(3)	Establecimiento y administración de claves criptográficas | Claves asimétricas	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12(3)	Establecimiento y administración de claves criptográficas | Claves asimétricas	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-12	Establecimiento y administración de claves criptográficas	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-12	Establecimiento y administración de claves criptográficas	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
SC-13	Protección criptográfica	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que los AWS CodeBuild artefactos estén cifrados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
SC-13	Protección criptográfica	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-13	Protección criptográfica	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.
SC-13	Protección criptográfica	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-13	Protección criptográfica	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
SC-13	Protección criptográfica	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-13	Protección criptográfica	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
SC-13	Protección criptográfica	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
SC-13	Protección criptográfica	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SC-13	Protección criptográfica	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-13	Protección criptográfica	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
SC-13	Protección criptográfica	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
SC-13	Protección criptográfica	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
SC-13	Protección criptográfica	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-13	Protección criptográfica	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23(3)	Autenticidad de sesión | Identific adores de sesión únicos generados por el sistema	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
SC-23(3)	Autenticidad de sesión | Identific adores de sesión únicos generados por el sistema	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23(3)	Autenticidad de sesión | Identific adores de sesión únicos generados por el sistema	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
SC-23(3)	Autenticidad de sesión | Identific adores de sesión únicos generados por el sistema	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23(3)	Autenticidad de sesión | Identific adores de sesión únicos generados por el sistema	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-23(3)	Autenticidad de sesión | Identific adores de sesión únicos generados por el sistema	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23(3)	Autenticidad de sesión | Identific adores de sesión únicos generados por el sistema	elb 2- acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-23(3)	Autenticidad de sesión | Identific adores de sesión únicos generados por el sistema	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23(3)	Autenticidad de sesión | Identific adores de sesión únicos generados por el sistema	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23(5)	Autenticidad de sesión | Autoridades de certificación autorizadas	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23(5)	Autenticidad de sesión | Autoridades de certificación autorizadas	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23	Autenticidad de sesión	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-23	Autenticidad de sesión	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23	Autenticidad de sesión	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
SC-23	Autenticidad de sesión	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23	Autenticidad de sesión	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-23	Autenticidad de sesión	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23	Autenticidad de sesión	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23	Autenticidad de sesión	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
SC-23	Autenticidad de sesión	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-23	Autenticidad de sesión	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SC-28(1)	Protección de la información en reposo | Protección criptográfica	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
SC-28(1)	Protección de la información en reposo | Protección criptográfica	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.
SC-28(1)	Protección de la información en reposo | Protección criptográfica	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
SC-28(1)	Protección de la información en reposo | Protección criptográfica	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	api-gw-cache-enabled-y cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28(1)	Protección de la información en reposo | Protección criptográfica	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
SC-28(1)	Protección de la información en reposo | Protección criptográfica	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SC-28(1)	Protección de la información en reposo | Protección criptográfica	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
SC-28(1)	Protección de la información en reposo | Protección criptográfica	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28(1)	Protección de la información en reposo | Protección criptográfica	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(1)	Protección de la información en reposo | Protección criptográfica	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28(3)	Protección de la información en reposo | Claves criptográficas	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
SC-28(3)	Protección de la información en reposo | Claves criptográficas	cmk-backing-key-rotation-activado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.
SC-28	Protección de la información en reposo	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	Protección de la información en reposo	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	Protección de la información en reposo	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	api-gw-cache-enabled-y cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	Protección de la información en reposo	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
SC-28	Protección de la información en reposo	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SC-28	Protección de la información en reposo	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
SC-28	Protección de la información en reposo	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
SC-28	Protección de la información en reposo	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-28	Protección de la información en reposo	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-36(2)	Procesamiento y almacenamiento distribuidos | Sincronización	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-36	Procesamiento y almacenamiento distribuidos	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-36	Procesamiento y almacenamiento distribuidos	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-36	Procesamiento y almacenamiento distribuidos	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SC-36	Procesamiento y almacenamiento distribuidos	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(2)	Corrección de defectos | Estado automatizado de la corrección de defectos	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(2)	Corrección de defectos | Estado automatizado de la corrección de defectos	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(2)	Corrección de defectos | Estado automatizado de la corrección de defectos	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(3)	Corrección de defectos | Tiempo de corrección de defectos y parámetros de referencia para las acciones correctivas	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(3)	Corrección de defectos | Tiempo de corrección de defectos y parámetros de referencia para las acciones correctivas	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(3)	Corrección de defectos | Tiempo de corrección de defectos y parámetros de referencia para las acciones correctivas	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
SI-2(4)	Corrección de defectos | Herramientas automatizadas de administración de parches	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(4)	Corrección de defectos | Herramientas automatizadas de administración de parches	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(4)	Corrección de defectos | Herramientas automatizadas de administración de parches	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(5)	Corrección de defectos | Actualizaciones automáticas de software y firmware	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(5)	Corrección de defectos | Actualizaciones automáticas de software y firmware	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2(5)	Corrección de defectos | Actualizaciones automáticas de software y firmware	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	Corrección de defectos	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	Corrección de defectos	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	Corrección de defectos	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	Corrección de defectos	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	Corrección de defectos	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	Corrección de defectos	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
SI-2	Corrección de defectos	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	Corrección de defectos	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-2	Corrección de defectos	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3(8)	Protección contra códigos maliciosos | Detección de comandos no autorizados	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3(8)	Protección contra códigos maliciosos | Detección de comandos no autorizados	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3(8)	Protección contra códigos maliciosos | Detección de comandos no autorizados	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3(8)	Protección contra códigos malicioso s | Detección de comandos no autorizados	s3- event-notification s-enabled	Las notificaciones de eventos de Amazon S3 pueden alertar al personal pertinente de cualquier modificac ión accidental o intencionada en los objetos de su bucket. Algunos ejemplos de alertas son: creación de un objeto nuevo, eliminación de objetos, restauración de objetos, objetos perdidos o replicados.
SI-3(8)	Protección contra códigos malicioso s | Detección de comandos no autorizados	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3(8)	Protección contra códigos maliciosos | Detección de comandos no autorizados	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3(8)	Protección contra códigos maliciosos | Detección de comandos no autorizados	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
SI-3(8)	Protección contra códigos maliciosos | Detección de comandos no autorizados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3(8)	Protección contra códigos maliciosos | Detección de comandos no autorizados	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3(8)	Protección contra códigos maliciosos | Detección de comandos no autorizados	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-3(8)	Protección contra códigos malicioso s | Detección de comandos no autorizados	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(1)	Monitoreo del sistema | Sistema de detección de intrusos en todo el sistema	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(2)	Monitoreo del sistema | Herramientas y mecanismos automatizados para el análisis en tiempo real	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(4)	Monitoreo del sistema | Tráfico de comunicaciones entrantes y salientes	s3- event-notifications-enabled	Las notificaciones de eventos de Amazon S3 pueden alertar al personal pertinente de cualquier modificación accidental o intencionada en los objetos de su bucket. Algunos ejemplos de alertas son: creación de un objeto nuevo, eliminación de objetos, restauración de objetos, objetos perdidos o replicados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(4)	Monitoreo del sistema | Tráfico de comunicaciones entrantes y salientes	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(5)	Monitoreo del sistema | Alertas generadas por el sistema	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(5)	Monitoreo del sistema | Alertas generadas por el sistema	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
SI-4(5)	Monitoreo del sistema | Alertas generadas por el sistema	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(12)	Monitoreo del sistema | Alertas automatizadas generadas por la organización	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(13)	Monitoreo del sistema | Análisis de patrones de tráfico y eventos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(20)	Monitoreo del sistema | Usuarios con privilegios	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(20)	Monitoreo del sistema | Usuarios con privilegios	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(20)	Monitoreo del sistema | Usuarios con privilegios	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
SI-4(20)	Monitoreo del sistema | Usuarios con privilegios	cloud-trail-cloud-watch-habilitados para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(20)	Monitoreo del sistema | Usuarios con privilegios	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(20)	Monitoreo del sistema | Usuarios con privilegios	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
SI-4(20)	Monitoreo del sistema | Usuarios con privilegios	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(20)	Monitoreo del sistema | Usuarios con privilegios	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(20)	Monitoreo del sistema | Usuarios con privilegios	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(22)	Monitoreo del sistema | Servicios de red no autorizados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4(25)	Monitoreo del sistema | Optimización del análisis del tráfico de red	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	Monitoreo del sistema	s3- event-notification s-enabled	Las notificaciones de eventos de Amazon S3 pueden alertar al personal pertinente de cualquier modificac ión accidental o intencionada en los objetos de su bucket. Algunos ejemplos de alertas son: creación de un objeto nuevo, eliminación de objetos, restauración de objetos, objetos perdidos o replicados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	Monitoreo del sistema	cloud-trail-log-file-habilitado para validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-4	Monitoreo del sistema	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(1)	Integridad del software, el firmware y la información | Controles de integrida d	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(3)	Integridad del software, el firmware y la información | Herramientas de integridad administr adas centralmente	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales almacenados, asegúrese de que los artefactos estén cifrados. AWS CodeBuild
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(6)	Integridad del software, el firmware y la información | Protección criptográfica	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(7)	Integridad del software, el firmware y la información | Integración de la detección y la respuesta	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-7(8)	Integridad del software, el firmware y la información | Capacidad de auditoría para eventos significativos	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	Administración y retención de la información	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	Administración y retención de la información	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	Administración y retención de la información	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	Administración y retención de la información	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	Administración y retención de la información	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	Administración y retención de la información	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-12	Administración y retención de la información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	s3- version-lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	elasticache-redis-cluster-automatic-comprobación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-13(5)	Prevención de fallos predecibles | Capacidad de conmutación por error	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-20	Contaminación	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
SI-20	Contaminación	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
SI-20	Contaminación	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el NIST 800-53 rev. 5.

Prácticas operativas recomendadas para NIST 800 171

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el NIST 800-171 y las reglas de AWS Config administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles NIST 800-171. Un control del NIST 800-171 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	usuarios autorizados o a los dispositivos (incluidos otros sistemas).		específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizad os o a los dispositi vos (incluidos otros sistemas).	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.1	Limitar el acceso al sistema a los usuarios autorizados, a los procesos que actúan en nombre de los usuarios autorizados o a los dispositivos (incluidos otros sistemas).	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.2	Limitar el acceso al sistema a los tipos de transacciones y funciones que los usuarios autorizados pueden ejecutar.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3	Controlar el flujo de la CUI de acuerdo con las autorizaciones aprobadas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.4	Separar las funciones de las personas para reducir el riesgo de actividad maliciosa sin colusión.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	efs-access-point-enforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-group-has-users-compruebe	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegios específicas.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.5	Emplear el principio de privilegio mínimo, incluidas las funciones de seguridad y las cuentas con privilegi os específicas.	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.6	Usar las cuentas o funciones sin privilegios al acceder a las funciones sin seguridad.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y auditen la ejecución de dichas funciones.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y auditen la ejecución de dichas funciones.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y auditen la ejecución de dichas funciones.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y auditen la ejecución de dichas funciones.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y auditen la ejecución de dichas funciones.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y auditen la ejecución de dichas funciones.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.7	Evitar que los usuarios sin privilegios ejecuten funciones con privilegios y auditen la ejecución de dichas funciones.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.12	Monitorear y controlar las sesiones de acceso remoto.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	elb 2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1.13	Emplear mecanismos criptográficos para proteger la confidencialidad de las sesiones de acceso remoto.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	subnet-auto-assign-public-ip-deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.14	Dirigir el acceso remoto desde puntos de control de acceso administrados.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearch Permite un control de acceso al dominio basado en funciones, así como una seguridad a nivel de índices, documentos y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	s3-: bucket-level-public-access prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.20	Verificar control/limit las conexiones y el uso de sistemas externos.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	api-gw-execution-l ogging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y transmitidos a Amazon CloudWatc h Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditoría s de seguridad y acceso, y pueden ayudar a diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1	Crear y retener los registros de auditoría del sistema si son necesarios para habilitar el monitoreo , los análisis, la investigación y la gestión de informes de actividad del sistema ilegal, no autorizada o inapropia da.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.
3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	api-gw-execution-l ogging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Garantizar que las acciones de usuarios del sistema individua les se puedan rastrear de forma unívoca hasta los usuarios para que se les pueda responsabilizar de sus acciones.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.4	Alertar sobre el evento de un error en el proceso de auditoría.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.4	Alertar sobre el evento de un error en el proceso de auditoría.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.5	Relacionar los procesos de revisión, análisis y gestión de informes de auditoría para investigar y responder a los indicios de actividad inapropiada, sospechosa o inusual.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.5	Relacionar los procesos de revisión, análisis y gestión de informes de auditoría para investigar y responder a los indicios de actividad inapropiada, sospechosa o inusual.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
3.3.8	Proteger la informaci ón de auditoría y las herramientas de auditoría de todo acceso, modificac ión y eliminación no autorizadas.	s3- bucket-default-loc k-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.8	Proteger la información de auditoría y las herramientas de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.8	Proteger la información de auditoría y las herramientas de auditoría de todo acceso, modificación y eliminación no autorizadas.	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.8	Proteger la información de auditoría y las herramientas de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.8	Proteger la informaci ón de auditoría y las herramientas de auditoría de todo acceso, modificac ión y eliminación no autorizadas.	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.8	Proteger la información de auditoría y las herramientas de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
3.3.8	Proteger la información de auditoría y las herramientas de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.8	Proteger la informaci ón de auditoría y las herramientas de auditoría de todo acceso, modificac ión y eliminación no autorizadas.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.8	Proteger la información de auditoría y las herramientas de auditoría de todo acceso, modificación y eliminación no autorizadas.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.1	Establecer y mantener configura ciones de referenci a e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectiv os.	ec2- -eni-periódico security-group-att ached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.1	Establecer y mantener configura ciones de referenci a e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectiv os.	ec2- instance-managed-by-systems-administrador	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.1	Establecer y mantener configuraciones de referencia e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectivos.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.1	Establecer y mantener configura ciones de referenci a e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectiv os.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.1	Establecer y mantener configura ciones de referenci a e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectiv os.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.1	Establecer y mantener configura ciones de referenci a e inventarios de los sistemas organizativos (incluido el hardware, software, firmware y la documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectiv os.	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizado s EIPs en su entorno.
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
3.4.6	Emplear el principio de funcionalidad mínima al configura r sistemas organizat ivos para proporcionar solo las capacidades esenciales.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.6	Emplear el principio de funcionalidad mínima al configurar sistemas organizativos para proporcionar solo las capacidades esenciales.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.7	Restringir, deshabilitar y evitar el uso de funciones, puertos, protocolos o servicios no esenciales.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.7	Restringir, deshabilitar y evitar el uso de funciones, puertos, protocolos o servicios no esenciales.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.7	Restringir, deshabilitar y evitar el uso de funciones, puertos, protocolos o servicios no esenciales.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.7	Restringir, deshabilitar y evitar el uso de funciones, puertos, protocolos o servicios no esenciales.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.9	Controlar y monitorear el software instalado por el usuario.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.9	Controlar y monitorear el software instalado por el usuario.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de la organización.	efs-access-point-e nforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configura da en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de la organización.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.2	Autenticar (o verificar) las identidades de aquellos usuarios, procesos o dispositi vos como requisito previo para permitir el acceso a los sistemas de la organización.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.3	Usar la autenticación multifactor para el acceso local y de red a cuentas con privilegios y para el acceso de red a cuentas sin privilegios.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.3	Usar la autenticación multifactor para el acceso local y de red a cuentas con privilegios y para el acceso de red a cuentas sin privilegios.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.3	Usar la autenticación multifactor para el acceso local y de red a cuentas con privilegios y para el acceso de red a cuentas sin privilegios.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.3	Usar la autenticación multifactor para el acceso local y de red a cuentas con privilegios y para el acceso de red a cuentas sin privilegios.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.5	Impedir la reutilización de los identificadores durante un período definido.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.6	Deshabilitar los identificadores tras un período definido de inactividad.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.7	Forzar una complejidad de contraseña mínima y cambiar los caracteres cuando se crean nuevas contraseñas.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.8	Prohibir la reutilización de contraseñas para un número específico de generaciones.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.10	Almacenar y transmitir únicamente contraseñ as protegidas criptográficamente.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
3.5.10	Almacenar y transmitir únicamente contraseñ as protegidas criptográficamente.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.10	Almacenar y transmitir únicamente contraseñ as protegidas criptográficamente.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
3.5.10	Almacenar y transmitir únicamente contraseñ as protegidas criptográficamente.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.10	Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1	Establecer una capacidad operativa de gestión de incidentes para los sistemas organizativos que incluya actividad es de preparación, detección, análisis, contención, recuperac ión y respuesta del usuario.	guardduty-non-arch ived-findings	Amazon le GuardDuty ayuda a comprende r el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasifica ciones para determina r las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1	Establecer una capacidad operativa de gestión de incidentes para los sistemas organizativos que incluya actividad es de preparación, detección, análisis, contención, recuperac ión y respuesta del usuario.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1	Establecer una capacidad operativa de gestión de incidentes para los sistemas organizativos que incluya actividad es de preparación, detección, análisis, contención, recuperac ión y respuesta del usuario.	cloudwatch-alarm-a ction-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluació n. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1	Establecer una capacidad operativa de gestión de incidentes para los sistemas organizativos que incluya actividad es de preparación, detección, análisis, contención, recuperac ión y respuesta del usuario.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11.2	Analizar en busca de vulnerabilidades de los sistemas organizativos y las aplicaciones de forma periódica y al identificar nuevas vulnerabilidades que afecten al sistema.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11.2	Analizar en busca de vulnerabilidades de los sistemas organizativos y las aplicaciones de forma periódica y al identificar nuevas vulnerabilidades que afecten al sistema.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11.3	Remediar las vulnerabilidades de acuerdo con las evaluaciones de riesgo.	guardduty-non-archived-findings	Amazon le GuardDuty ayuda a comprender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.1	Monitorear, controlar y proteger las comunicaciones (es decir, la información transmitida o recibida por los sistemas de la organización) en el perímetro externo y el perímetro interno clave de los sistemas de la organización.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearch Permite un control de acceso al dominio basado en funciones, así como una seguridad a nivel de índices, documentos y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarroll o de software y principios de ingenierí a de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- -prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	subnet-auto-assign-public-ip-deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.2	Emplear diseños arquitectónicos, técnicas de desarrollo de software y principios de ingeniería de software para promocionar la seguridad efectiva de la información dentro de los sistemas organizativos.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.6	Denegar el tráfico de comunicaciones de red de forma predeterminada y permitir el tráfico de comunicaciones de red por excepción (es decir, denegar todo, permitir por excepción).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.6	Denegar el tráfico de comunicaciones de red de forma predeterminada y permitir el tráfico de comunicaciones de red por excepción (es decir, denegar todo, permitir por excepción).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.6	Denegar el tráfico de comunicaciones de red de forma predeterminada y permitir el tráfico de comunicaciones de red por excepción (es decir, denegar todo, permitir por excepción).	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.13.8	Implementar mecanismos criptográficos para evitar la divulgación no autorizada de la CUI durante la transmisión a menos que esté protegido de otra manera con medidas de protección físicas alternativas.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.10	Establecer y administrar claves criptográficas para la criptografía empleada en los sistemas organizativos.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
3.13.10	Establecer y administrar claves criptográficas para la criptografía empleada en los sistemas organizativos.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
3.13.16	Proteger la confidencialidad de la CUI en reposo.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
3.13.16	Proteger la confidencialidad de la CUI en reposo.	s3- bucket-default-lock-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
3.13.16	Proteger la confidencialidad de la CUI en reposo.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus AWS CloudTrail registros.
3.13.16	Proteger la confidencialidad de la CUI en reposo.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
3.13.16	Proteger la confidencialidad de la CUI en reposo.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
3.13.16	Proteger la confidencialidad de la CUI en reposo.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
3.13.16	Proteger la confidencialidad de la CUI en reposo.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.16	Proteger la confidencialidad de la CUI en reposo.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
3.13.16	Proteger la confidencialidad de la CUI en reposo.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.1	Identificar, notificar y corregir los defectos de la información y de los sistemas de manera oportuna.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.1	Identificar, notificar y corregir los defectos de la información y de los sistemas de manera oportuna.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.2	Proporcionar protección contra código malicioso en las ubicaciones adecuadas dentro de los sistemas de la organización.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.2	Proporcionar protección contra código malicioso en las ubicaciones adecuadas dentro de los sistemas de la organización.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.3	Monitorear las alertas y avisos de seguridad del sistema y tomar medidas.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferredMaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
3.14.4	Actualizar los mecanismos de protección contra códigos maliciosos cuando haya nuevas versiones disponibles.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizat ivos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicacio nes web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizat ivos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizat ivos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizat ivos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizat ivos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizativos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizat ivos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6	Monitorear los sistemas organizat ivos, incluido el tráfico de la comunicación entrante y saliente, para detectar ataques e indicadores de ataques potenciales.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizativos.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7	Identificar el uso no autorizado de sistemas organizat ivos.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el NIST 800 171.

Prácticas operativas recomendadas para NIST 800 172

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el NIST 800-172 y las reglas de AWS Config administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a

uno o más controles NIST 800-172. Un control del NIST 800-172 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1.3e	Emplear [Asignación: soluciones de	api-gw-ssl-enabled	Asegúrese de que las etapas de la API

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.		de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	alb-desync-mode-check	Para ayudar a proteger las aplicaciones contra las vulnerabilidades de desincronización HTTP, asegurar que el modo de mitigación de desincronización HTTP esté habilitado en los equilibradores de carga de aplicación. Los problemas de desincronización de HTTP pueden provocar el contrabando de solicitudes y hacer que sus aplicaciones sean vulnerables al envenenamiento de las colas de solicitudes o de la caché. La mitigación de desincronización incluye modos monitoreados, defensivos y más estrictos. El modo defensivo es el modo predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	clb-desync-mode-check	Para ayudar a proteger las aplicaciones contra las vulnerabilidades de desincronización HTTP, asegurar que el modo de mitigación de desincronización HTTP esté habilitado en los equilibradores de carga de aplicación. Los problemas de desincronización de HTTP pueden provocar el contrabando de solicitudes y hacer que sus aplicaciones sean vulnerables al envenenamiento de las colas de solicitudes o de la caché. La mitigación de desincronización incluye modos monitoreados, defensivos y más estrictos. El modo defensivo es el modo predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	ec2- token-hop-limit-check	Asegúrese de que la respuesta HTTP PUT del servicio de metadatos de instancias (IMDS) esté restringida a la instancia de Amazon Elastic Compute Cloud (Amazon EC2). Con IMDSv2, la respuesta PUT que contiene el token secreto de forma predeterminada no puede viajar fuera de la instancia, ya que el límite de saltos de respuesta de metadatos está establecido en 1 (valor predeterminado de Config). Si este valor es superior a 1, el token puede salir de la instancia EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1.3e	Emplear [Asignación: soluciones de transferencia de información seguras definidas por la organización] para controlar los flujos de información entre los dominios de seguridad de los sistemas conectados.	nacl-no-unrestricted-ssh-rdp	El acceso a los puertos de administración remota de servidores de las listas de control de acceso a la red (NACLs), como el puerto 22 (SSH) y el puerto 3389 (RDP), no debe ser de acceso público, ya que esto puede permitir el acceso no deseado a los recursos de la VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1e	Ofrezca una capacitación de sensibilización [asignación: frecuencia definida por la organización] centrada en reconocer y responder a las amenazas derivadas de la ingeniería social, los actores de amenazas avanzadas y persistentes, las infracciones y los comportamientos sospechosos; actualice la formación [asignación: frecuencia definida por la organización] o cuando se produzcan cambios significativos en la amenaza.	security-awareness-program-exists (comprobación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.2e	Use mecanismos automatizados para detectar componentes del sistema mal configurados o no autorizados; tras la detección, [seleccione (uno o más): retire los componentes; coloque los componentes en una red de cuarentena o remediación] para facilitar la aplicación de parches, la reconfiguración u otras medidas de mitigación.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.2e	Use mecanismos automatizados para detectar componentes del sistema mal configurados o no autorizados; tras la detección, [seleccione (uno o más): retire los componentes; coloque los componentes en una red de cuarentena o remediación] para facilitar la aplicación de parches, la reconfiguración u otras medidas de mitigación.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.2e	Use mecanismos automatizados para detectar componentes del sistema mal configurados o no autorizados; tras la detección, [seleccione (uno o más): retire los componentes; coloque los componentes en una red de cuarentena o remediación] para facilitar la aplicación de parches, la reconfiguración u otras medidas de mitigación.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.2e	Use mecanismos automatizados para detectar componentes del sistema mal configurados o no autorizados; tras la detección, [seleccione (uno o más): retire los componentes; coloque los componentes en una red de cuarentena o remediación] para facilitar la aplicación de parches, la reconfiguración u otras medidas de mitigación.	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.3e	Emplee herramientas automatizadas de descubrimiento y administración para mantener un inventario completo up-to-date, preciso y fácilmente disponible de los componentes del sistema.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.3e	Utilice herramientas automatizadas de descubrimiento y administración para mantener un inventario completo up-to-date, preciso y fácilmente disponible de los componentes del sistema.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.3e	Emplee herramientas automatizadas de descubrimiento y administración para mantener un inventario completo up-to-date, preciso y fácilmente disponible de los componentes del sistema.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4.3e	Emplee herramientas automatizadas de descubrimiento y administración para mantener un inventario completo up-to-date, preciso y fácilmente disponible de los componentes del sistema.	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a monitorear los no utilizados EIPs en su entorno.
3.4.3e	Utilice herramientas automatizadas de descubrimiento y administración para mantener un inventario completo up-to-date, preciso y fácilmente disponible de los componentes del sistema.	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.2e	Emplee mecanismos automatizados para la generación, protección, rotación y administración de contraseñas para los sistemas y componentes del sistema que no admitan la autenticación multifactorial o la administración de cuentas complejas.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.2e	Emplee mecanismos automatizados para la generación, protección, rotación y administración de contraseñas para los sistemas y componentes del sistema que no admitan la autenticación multifactorial o la administración de cuentas complejas.	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.
3.5.2e	Emplee mecanismos automatizados para la generación, protección, rotación y administración de contraseñas para los sistemas y componentes del sistema que no admitan la autenticación multifactorial o la administración de cuentas complejas.	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.2e	Emplee mecanismos automatizados para la generación, protección, rotación y administración de contraseñas para los sistemas y componentes del sistema que no admitan la autenticación multifactorial o la administración de cuentas complejas.	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11.1e	Emplee [asignación: fuentes de inteligencia sobre amenazas definidas por la organización] como parte de una evaluación de riesgos para guiar y determine el desarrollo de los sistemas organizativos, las arquitecturas de seguridad, la selección de soluciones de seguridad, la supervisión, la búsqueda de amenazas y las actividades de respuesta y recuperación.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11.2e	Realizar actividades de búsqueda de ciberamenazas [selección (una o más): [asignación: frecuencia definida por la organización]; [asignación: evento definido por la organización]] para buscar indicadores de situaciones de riesgo en [asignación: sistemas definidos por la organización] y detectar, rastrear e interrumpir las amenazas que eluden los controles existentes.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.11.5e	Evaluar la eficacia de las solucione s de seguridad [asignación: frecuenci a definida por la organización] para abordar el riesgo previsto para los sistemas organizat ivos y la organizac ión en función de la información sobre amenazas actual y acumulada.	annual-risk-assess ment-performed (verificación de procesos)	Realice una evaluació n anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determina r la probabilidad y el impacto de los riesgos y and/or vulnerabi lidades identificados que afectan a una organización.
3.13.4e	Emplee [selecció n: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizat ivos y los component es del sistema.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selecció n: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizat ivos y los component es del sistema.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selecció n: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizat ivos y los component es del sistema.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
3.13.4e	Emplee [selecció n: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizat ivos y los component es del sistema.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	nacl-no-unrestricted-ssh-rdp	El acceso a los puertos de administración remota de servidores de las listas de control de acceso a la red (NACLs), como el puerto 22 (SSH) y el puerto 3389 (RDP), no debe ser de acceso público, ya que esto puede permitir el acceso no deseado a los recursos de la VPC.
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.13.4e	Emplee [selección: (una o más): [asignación: técnicas de aislamiento físico definidas por la organización]; [asignación: técnicas de aislamiento lógico definidas por la organización]] en los sistemas organizativos y los componentes del sistema.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.1e	Verifique la integrida d de [asignación: software crítico o esencial para la seguridad definido por la organización] mediante mecanismo s de raíz de confianza o firmas criptográ ficas.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.2e	Monitoree sistemas organizativos y componentes del sistema de forma regular en busca de comportam ientos anómalos o sospechosos.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
3.14.2e	Monitoree sistemas organizativos y componentes del sistema de forma regular en busca de comportam ientos anómalos o sospechosos.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.2e	Monitoree sistemas organizativos y componentes del sistema de forma regular en busca de comportam ientos anómalos o sospechosos.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.2e	Monitoree sistemas organizativos y componentes del sistema de forma regular en busca de comportam ientos anómalos o sospechosos.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.2e	Monitoree sistemas organizativos y componentes del sistema de forma regular en busca de comportamientos anómalos o sospechosos.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.2e	Monitoree sistemas organizativos y componentes del sistema de forma regular en busca de comportam ientos anómalos o sospechosos.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.2e	Monitoree sistemas organizativos y componentes del sistema de forma regular en busca de comportam ientos anómalos o sospechosos.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.6e	Utilice la información sobre los indicador es de amenazas y las mitigaciones efectivas obtenidas de [asignaci ón: organizaciones externas definidas por la organizac ión] para guiar e informar sobre la detección de intrusion es y la búsqueda de amenazas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7e	Verifique la exactitud de [asignación: componentes de software, firmware y hardware esenciales o críticos para la seguridad definidos por la organización] mediante [asignación: métodos o técnicas de verificación definidos por la organización].	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7e	Verifique la exactitud de [asignación: componentes de software, firmware y hardware esenciales o críticos para la seguridad definidos por la organización] mediante [asignación: métodos o técnicas de verificación definidos por la organización].	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7e	Verifique la exactitud de [asignación: componentes de software, firmware y hardware esenciales o críticos para la seguridad definidos por la organización] mediante [asignación: métodos o técnicas de verificación definidos por la organización].	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7e	Verifique la exactitud de [asignación: componentes de software, firmware y hardware esenciales o críticos para la seguridad definidos por la organización] mediante [asignación: métodos o técnicas de verificación definidos por la organización].	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administración de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independientes de sus servicios para usar la versión de plataforma más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.14.7e	Verifique la exactitud de [asignación: componentes de software, firmware y hardware esenciales o críticos para la seguridad definidos por la organización] mediante [asignación: métodos o técnicas de verificación definidos por la organización].	ecr-private-image-scanning-habilitado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el NIST 800 172.

Prácticas operativas recomendadas para NIST 800 181

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el NIST 800 181 y las reglas de Config AWS administradas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles NIST 800 181. Un control del NIST 800 181 puede estar relacionado con varias reglas

de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	elb-cross-zone-load-habilitado para el balanceo	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
T0008	Analice y planifique los cambios anticipados en los requisitos de capacidad de datos.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	opensearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon Elasticsearch Service (Amazon ES).
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
T0017	Aplique los principio s de la arquitect ura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibi lidad de la organizac ión.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0017	Aplique los principios de la arquitectura de seguridad orientada a los servicios para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de la organización.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0024	Recopile y mantenga los datos necesarios para cumplir con los informes de ciberseguridad del sistema.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0042	Coordínese con los analistas de ciberdefensa para gestionar y administrar la actualización de las reglas y firmas (por ejemplo, detection/protection sistemas de intrusión, antivirus y listas negras de contenido) para aplicaciones especializadas de ciberdefensa.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0047	Correlaciona los datos de los incidentes para identificar vulnerabilidades específicas y hacer recomendaciones que permitan una remediación rápida.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluidos los posibles fallosover/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluidos los posibles fallos. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluidos los posibles fallos. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones fundamentales del sistema y asegúrese de que los requisitos del sistema identifiq uen los requisito s adecuados de recuperación ante desastres y continuid ad de las operacion es, incluidos los posibles fallos. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	dynamodb-throughpu t-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/ write actividad que puede soportar cada tabla. DynamoDB utiliza esta informaci ón para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalm ente los parámetro s de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuid ad de las operacion es, incluidos los posibles fallosove r/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluidos los posibles fallosover/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación en caso de desastre y continuidad de las operaciones, incluyendo cualquier fallo apropiado. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuidad de las operaciones, incluyendo cualquier fallo apropiado over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación en caso de desastre y continuidad de las operaciones, incluyendo cualquier fallo apropiado over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación en caso de desastre y continuidad de las operaciones, incluyendo cualquier fallo apropiado over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones fundamentales del sistema y asegúrese de que los requisitos del sistema identifiq uen los requisito s adecuados de recuperación ante desastres y continuid ad de las operacion es, incluidos los posibles fallos. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	backup-plan-min-fr equency-and-min-re tention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) y requiredF requencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
T0051	Defina los niveles adecuados de disponibilidad del sistema en función de las funciones críticas del sistema y asegúrese de que los requisitos del sistema identifiquen los requisitos adecuados de recuperación ante desastres y continuid ad de las operacion es, incluidos los posibles fallosove r/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0065	Desarrolle e implemente procedimientos de copia de seguridad y recuperación de redes.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
T0070	Desarrolle planes de recuperación de desastres y continuid ad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0070	Desarrolle planes de recuperación de desastres y continuidad de las operaciones para los sistemas en desarrollo y garantice las pruebas antes de que los sistemas entren en un entorno de producción.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0086	Asegúrese de que la aplicación de los parches de seguridad para los productos comerciales integrados en el diseño del sistema cumpla con los plazos dictados por la autoridad de gestión para el entorno operativo previsto.	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0086	Asegúrese de que la aplicación de los parches de seguridad para los productos comerciales integrados en el diseño del sistema cumpla con los plazos dictados por la autoridad de gestión para el entorno operativo previsto.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0086	Asegúrese de que la aplicación de los parches de seguridad para los productos comerciales integrados en el diseño del sistema cumpla con los plazos dictados por la autoridad de gestión para el entorno operativo previsto.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0086	Asegúrese de que la aplicación de los parches de seguridad para los productos comerciales integrados en el diseño del sistema cumpla con los plazos dictados por la autoridad de gestión para el entorno operativo previsto.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0110	Identifique y and/or determine si un incidente de seguridad es indicativo de una infracción de la ley que requiere una acción legal específica.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0110	Identifique y and/or determine si un incidente de seguridad es indicativo de una infracción de la ley que requiere una acción legal específica.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0110	Identifique y and/ or determine si un incidente de seguridad es indicativ o de una infracción de la ley que requiere una acción legal específica.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0128	Integre capacidades automatizadas para actualizar o parchear el software del sistema cuando resulte práctico y desarrolle procesos y procedimientos para actualizar y aplicar parches manualmente al software del sistema en función de los requisitos actuales y proyectados del cronograma de parches para el entorno operativo del sistema.	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0128	Integre capacidades automatizadas para actualizar o parchear el software del sistema cuando resulte práctico y desarrolle procesos y procedimientos para actualizar y aplicar parches manualmente al software del sistema en función de los requisitos actuales y proyectados del cronograma de parches para el entorno operativo del sistema.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0128	Integre capacidad es automatizadas para actualizar o parchear el software del sistema cuando resulte práctico y desarrolle procesos y procedimientos para actualizar y aplicar parches manualmen te al software del sistema en función de los requisitos actuales y proyectad os del cronograma de parches para el entorno operativo del sistema.	elastic-beanstalk-managed-updates-ha bilitado	La activación de las actualizaciones de plataforma gestionad as para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correccio nes, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomenda da para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0128	Integre capacidades automatizadas para actualizar o parchear el software del sistema cuando resulte práctico y desarrolle procesos y procedimientos para actualizar y aplicar parches manualmente al software del sistema en función de los requisitos actuales y proyectados del cronograma de parches para el entorno operativo del sistema.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon Elasticsearch Service (Amazon ES) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de ES dentro de una Amazon VPC garantiza una comunicación segura entre Amazon ES y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0144	Administre las cuentas, los derechos de red y el acceso a los sistemas y equipos.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0151	Supervise y evalúe la eficacia de las medidas de seguridad cibernética de la empresa para asegurarse de que proporcionen el nivel de protección previsto.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0151	Supervise y evalúe la eficacia de las medidas de seguridad cibernética de la empresa para asegurarse de que proporcionen el nivel de protección previsto.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0151	Supervise y evalúe la eficacia de las medidas de seguridad cibernética de la empresa para asegurarse de que proporcionen el nivel de protección previsto.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que establezcas el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	redshift-cluster-public-access-marcar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0152	Supervise y mantenga las bases de datos para garantizar un rendimiento óptimo.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0153	Supervise la capacidad y el rendimiento de la red.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0153	Supervise la capacidad y el rendimiento de la red.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
T0153	Supervise la capacidad y el rendimiento de la red.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0153	Supervise la capacidad y el rendimiento de la red.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	cw-loggroup-retention-period-compruebe	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta informaci ón para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalm ente los parámetro s de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0154	Supervise y notifique el uso de los activos y recursos de la gestión del conocimiento.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0156	Supervise y haga recomendaciones en relación con la administración de la configuración.	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0156	Supervise y haga recomendaciones en relación con la administración de la configuración.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0156	Supervise y haga recomendaciones en relación con la administración de la configuración.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0156	Supervise y haga recomendaciones en relación con la administración de la configuración.	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0156	Supervise y haga recomendaciones en relación con la administración de la configuración.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0156	Supervise y haga recomendaciones en relación con la administración de la configuración.	elastic-beanstalk-managed-updates-activado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0156	Supervise y haga recomendaciones en relación con la administración de la configuración.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0156	Supervise y haga recomendaciones en relación con la administración de la configuración.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0156	Supervise y haga recomendaciones en relación con la administración de la configuración.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0160	Corrija mediante parches las vulnerabilidades de la red para garantizar que la información esté protegida contra terceros.	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0160	Corrija mediante parches las vulnerabilidades de la red para garantizar que la información esté protegida contra terceros.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0160	Corrija mediante parches las vulnerabilidades de la red para garantizar que la información esté protegida contra terceros.	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0162	Realice copias de seguridad y recuperación de las bases de datos para garantizar la integridad de los datos.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0166	Realice una correlación de eventos utilizando información recopilada de diversas fuentes dentro de la empresa para conocer la situación y determinar la eficacia de un ataque observado.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0168	Realice una comparación de hash con una base de datos establecida.	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibi lidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon Elasticsearch Service (Amazon ES) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de ES dentro de una Amazon VPC garantiza una comunicación segura entre Amazon ES y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0195	Proporcione un flujo gestionado de información relevante (a través de portales web u otros medios) en función de los requisitos de la misión.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0215	Reconozca una posible infracción de seguridad y tome las medidas adecuadas para denunciar el incidente, según sea necesario.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0244	Compruebe que las posturas software/network/system de seguridad de las aplicaciones se implementen según lo indicado, documente las desviaciones y recomiende las acciones necesarias para corregirlas.	cloud-trail-log-file-habilitada para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0244	Verifique que las posturas software/network/system de seguridad de las aplicaciones se implementen según lo indicado, documente las desviaciones y recomiende las acciones necesarias para corregir esas desviaciones.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0244	Compruebe que las posturas software/ network/system de seguridad de las aplicaciones se implementan según lo indicado, documente las desviaciones y recomiende las acciones necesarias para corregirlas.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0258	Detecte, identifique y alerte oportunam ente sobre posibles ataques o intrusiones, actividades anómalas y actividades de uso indebido, y distinga estos incidentes y eventos de actividad es benignas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0259	Utilice herramientas de ciberdefensa para monitorear y analizar continuamente la actividad del sistema con el fin de identificar actividades maliciosa s.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple ubicaciones, niveles de defensa, solidez de la seguridad).	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, defensas en capas, solidez de la seguridad).	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon Elasticsearch Service (Amazon ES) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de ES dentro de una Amazon VPC garantiza una comunicación segura entre Amazon ES y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple ubicaciones, niveles de defensa, solidez de la seguridad).	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple ubicaciones, niveles de defensa, solidez de la seguridad).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple ubicaciones, niveles de defensa, solidez de la seguridad).	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, capas de defensa, solidez de la seguridad).	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0262	Emplee defense-in-depth principios y prácticas aprobados (por ejemplo, defense-in-multiple lugares, niveles de defensa, solidez de la seguridad).	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos tools/technologies relacionados con la ciberseguridad.	account-part-of-or ganizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantiza r que las cuentas cumplan con las normas. La falta de gobernanza centraliz ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevas tools/technologies relacionadas con la ciberseguridad.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevas tools/tec hnologies relaciona das con la cibersegu ridad.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitud es web en función de las reglas y condicion es de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevas tools/tec hnologies relaciona das con la cibersegu ridad.	autoscaling-launch -config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
T0284	Diseñe y desarrolle nuevas áreas tools/ technologies relaciona das con la cibersegu ridad.	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñar y desarrollar nuevas áreas tools/ technologies relacionadas con la ciberseguridad.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseña y desarroll a nuevos tools/tec hnologies temas relacionados con la ciberseguridad.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevas tools/technologies relacionadas con la ciberseguridad.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseña y desarroll a nuevos tools/tec hnologies temas relacionados con la ciberseguridad.	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
T0284	Diseñe y desarrolle nuevos tools/technologies productos relacionados con la ciberseguridad.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos tools/technologies relacionados con la ciberseguridad.	rds-automatic-mino r-version-habilitado para la actualización	Habilite las actualiza ciones automátic as de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundari as del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correccio nes de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos relacionados con la tools/technologies ciberseguridad.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos tools/technologies relacionados con la ciberseguridad.	s3- account-level-publ ic-access -bloques- periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle novedades tools/technologies relacionadas con la ciberseguridad.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
T0284	Diseñe y desarrolle nuevos artículos relacionados con tools/technologies la ciberseguridad.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevas tools/tec hnologies relaciona das con la cibersegu ridad.	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos temas relacionados con tools/technologies la ciberseguridad.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos tools/tec hnologies relaciona dos con la cibersegu ridad.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositor io fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorizac ión de acceso a los repositorios de Bitbucket GitHub .
T0284	Diseña y desarrolla novedades relaciona das con tools/tec hnologies la cibersegu ridad.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevas tools/tec hnologies relaciona das con la cibersegu ridad.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
T0284	Diseñe y desarrolle nuevas relacionadas con tools/technologies la ciberseguridad.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevas tools/tec hnologies relaciona das con la cibersegu ridad.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos tools/technologies relacionados con la ciberseguridad.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
T0284	Diseña y desarroll a nuevos tools/tec hnologies temas relacionados con la ciberseguridad.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevos tools/technologies relacionados con la ciberseguridad.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0284	Diseñe y desarrolle nuevos productos tools/technologies relacionados con la ciberseguridad.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos temas relacionados con tools/technologies la ciberseguridad.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos tools/technologies relacionados con la ciberseguridad.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevas tools/technologies relacionadas con la ciberseguridad.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevos temas tools/ technologies relacionados con la ciberseguridad.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevas tools/technologies relacionadas con la ciberseguridad.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevos artículos tools/technologies relacionados con la ciberseguridad.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseña y desarroll a nuevos tools/tec hnologies temas relacionados con la ciberseguridad.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevas tools/technologies relacionadas con la ciberseguridad.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle novedades tools/technologies relacionadas con la ciberseguridad.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevas tools/tec hnologies relaciona das con la cibersegu ridad.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
T0284	Diseñe y desarrolle nuevas tools/technologies relacionadas con la ciberseguridad.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevos artículos tools/ technologies relacionados con la ciberseguridad.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon Elasticsearch Service (Amazon ES) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de ES dentro de una Amazon VPC garantiza una comunicación segura entre Amazon ES y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos temas relacionados con tools/technologies la ciberseguridad.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevas tools/tec hnologies relaciona das con la cibersegu ridad.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevas tools/technologies relacionadas con la ciberseguridad.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseña y desarrolla novedades relacionadas con tools/technologies la ciberseguridad.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos tools/technologies relacionados con la ciberseguridad.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos tools/technologies relacionados con la ciberseguridad.	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos tools/technologies relacionados con la ciberseguridad.	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevos productos tools/technologies relacionados con la ciberseguridad.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
T0284	Diseñe y desarrolle nuevos artículos tools/ technologies relaciona dos con la cibersegu ridad.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle nuevos artículos tools/ technologies relacionados con la ciberseguridad.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarrolle novedades tools/technologies relacionadas con la ciberseguridad.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevas tools/tec hnologies relaciona das con la cibersegu ridad.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0284	Diseñe y desarroll e nuevas tools/tec hnologies relaciona das con la cibersegu ridad.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube aseguránd ose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringi r el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibi lidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0306	Facilite la administración de incidentes, la administración del nivel de servicio, la administración de cambios, la administración de versiones, la administración de la continuidad y la administración de la disponibilidad para bases de datos y sistemas de administración de datos.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0306	Facilite la administración de incidentes, la administración del nivel de servicio, la administración de cambios, la administración de versiones, la administración de la continuidad y la administración de la disponibilidad para bases de datos y sistemas de administración de datos.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0306	Facilite la administración de incidentes, la administración del nivel de servicio, la administración de cambios, la administración de versiones, la administración de la continuidad y la administración de la disponibilidad para bases de datos y sistemas de administración de datos.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0314	Desarrolle un contexto de seguridad del sistema y un concepto de operaciones preliminar de seguridad del sistema (CONOPS) y defina los requisitos básicos de seguridad del sistema de acuerdo con los requisitos de ciberseguridad aplicables.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0314	Desarrolle un contexto de seguridad del sistema y un concepto de operaciones preliminar de seguridad del sistema (CONOPS) y defina los requisitos básicos de seguridad del sistema de acuerdo con los requisitos de ciberseguridad aplicables.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0314	Desarrolle un contexto de seguridad del sistema y un concepto de operaciones preliminar de seguridad del sistema (CONOPS) y defina los requisitos básicos de seguridad del sistema de acuerdo con los requisitos de ciberseguridad aplicables.	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0314	Desarrolle un contexto de seguridad del sistema y un concepto de operaciones preliminar de seguridad del sistema (CONOPS) y defina los requisitos básicos de seguridad del sistema de acuerdo con los requisitos de ciberseguridad aplicables.	ec-2 volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0314	Desarrolle un contexto de seguridad del sistema y un concepto de operaciones preliminar de seguridad del sistema (CONOPS) y defina los requisitos básicos de seguridad del sistema de acuerdo con los requisitos de ciberseguridad aplicables.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0314	Desarrolle un contexto de seguridad del sistema y un concepto de operaciones preliminar de seguridad del sistema (CONOPS) y defina los requisitos básicos de seguridad del sistema de acuerdo con los requisitos de ciberseguridad aplicables.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0333	Realice análisis e informes de tendencia s de ciberdefensa.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0333	Realice análisis e informes de tendencias de ciberdefensa.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0347	Evalúe la validez de los datos de origen y los hallazgos posteriores.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0358	Diseñe y desarroll e la funcionalidad de administración y gestión del sistema para usuarios con acceso privilegiado.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0358	Diseñe y desarrolle la funcionalidad de administración y gestión del sistema para usuarios con acceso privilegiado.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0358	Diseñe y desarroll e la funcionalidad de administración y gestión del sistema para usuarios con acceso privilegiado.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios del mínimo privilegio y la separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0358	Diseñe y desarrolle la funcionalidad de administración y gestión del sistema para usuarios con acceso privilegiado.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0358	Diseñe y desarroll e la funcionalidad de administración y gestión del sistema para usuarios con acceso privilegiado.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0358	Diseñe y desarrolle la funcionalidad de administración y gestión del sistema para usuarios con acceso privilegiado.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0358	Diseñe y desarrolle la funcionalidad de administración y gestión del sistema para usuarios con acceso privilegiado.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0358	Diseñe y desarroll e la funcionalidad de administración y gestión del sistema para usuarios con acceso privilegiado.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.
T0376	Establezca, asigne recursos, implement e y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	cloud-trail-cloud-watch-habilitada para guardar registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implemente y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0376	Establezca, asigne recursos, implement e y evalúe los programas de administración de la fuerza laboral cibernética de acuerdo con los requisitos de la organización.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
T0416	Habilite las aplicaciones con claves públicas aprovechando las bibliotecas de infraestructura de clave pública (PKI) existentes e incorporando funcionalidades de cifrado y administración de certificados cuando corresponda.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
T0421	Administre la indexación/catalogación, el almacenamiento y el acceso al conocimiento organizativo explícito (por ejemplo, documentos impresos o archivos digitales).	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-k now.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-know.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-know.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-know.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-know.	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-know.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-k now.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-k now	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-k now.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-k now.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-know.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-know.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-know.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-k now.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon Elasticsearch Service (Amazon ES) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de ES dentro de una Amazon VPC garantiza una comunicación segura entre Amazon ES y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y. need-to-know	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-k now.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-k now.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-k now.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0475	Evalúe los controles de acceso adecuados basándose en los principios del mínimo privilegio y need-to-k now.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimientos establecidos para garantizar la confidencialidad, integridad, disponibilidad, autenticación y no repudio.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimi entos establecidos para garantizar la confidencialidad, integridad, disponibi lidad, autenticación y no repudio.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimientos establecidos para garantizar la confidencialidad, integridad, disponibilidad, autenticación y no repudio.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimientos establecidos para garantizar la confidencialidad, integridad, disponibilidad, autenticación y no repudio.	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimientos establecidos para garantizar la confidencialidad, integridad, disponibilidad, autenticación y no repudio.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimi entos establecidos para garantizar la confidencialidad, integridad, disponibi lidad, autenticación y no repudio.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimi entos establecidos para garantizar la confidencialidad, integridad, disponibi lidad, autenticación y no repudio.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimi entos establecidos para garantizar la confidencialidad, integridad, disponibi lidad, autenticación y no repudio.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimi entos establecidos para garantizar la confidencialidad, integridad, disponibi lidad, autenticación y no repudio.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimientos establecidos para garantizar la confidencialidad, integridad, disponibilidad, autenticación y no repudio.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimi entos establecidos para garantizar la confidencialidad, integridad, disponibi lidad, autenticación y no repudio.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0489	Implemente medidas de seguridad del sistema de acuerdo con los procedimi entos establecidos para garantizar la confidencialidad, integridad, disponibi lidad, autenticación y no repudio.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0491	Instale y configure el hardware, el software y los equipos periféricos para los usuarios del sistema de acuerdo con los estándares de la organización.	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0491	Instale y configure el hardware, el software y los equipos periféricos para los usuarios del sistema de acuerdo con los estándares de la organización.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0491	Instale y configure el hardware, el software y los equipos periféricos para los usuarios del sistema de acuerdo con los estándares de la organización.	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0503	Supervise los orígenes de datos externos (por ejemplo, los sitios de proveedores de ciberseguridad, los equipos de respuesta a emergencias informáticas o Security Focus) para mantener actualiza da la situación de las amenazas de ciberseguridad y determinar qué problemas de seguridad pueden afectar a la empresa.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
T0509	Realice una evaluació n de los riesgos de seguridad de la información.	annual-risk-assess ment-performed (verificación de procesos)	Realice una evaluació n anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determina r la probabilidad y el impacto de los riesgos y and/or vulnerabi lidades identificados que afectan a una organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado de Amazon Elasticsearch Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	opensearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon Elasticsearch Service (Amazon ES).
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado de Amazon Elasticsearch Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	elasticsearch-encrypted-at-rest	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus dominios de Amazon Elasticsearch Service (Amazon ES).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	elb-acm-certificate-required	Dado que pueden existir datos confidenc iales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitad o para su Elastic Load Balancing. Use AWS Certifica te Manager para administrar, aprovisio nar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidades) para reducir las oportunidades de explotación.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitad o para su clúster de Amazon Redshift. Puesto que puede haber datos confidenc iales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0553	Aplique funciones de ciberseguridad (por ejemplo, cifrado, control de acceso y gestión de identidad es) para reducir las oportunidades de explotación.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS clave s (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.
T0557	Integre las funciones de administración clave relacionadas con el ciberespacio.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantiza r que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0557	Integre las funciones de administración clave relacionadas con el ciberespacio.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0576	Evalúe la inteligencia de todas las fuentes y recomiende objetivos para respaldar los objetivos de las operaciones cibernéticas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon Elasticsearch Service (Amazon ES) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de ES dentro de una Amazon VPC garantiza una comunicación segura entre Amazon ES y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitac ión del acceso a redes informáticas y digitales inalámbricas.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon Elasticsearch Service (Amazon ES) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de ES dentro de una Amazon VPC garantiza una comunicación segura entre Amazon ES y otros servicios dentro de la Amazon VPC sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0609	Realice la habilitación del acceso a redes informáticas y digitales inalámbricas.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0616	Realice exploraciones de redes y análisis de vulnerabilidades de los sistemas dentro de una red.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0686	Identifique las vulnerabilidades ante posibles amenazas.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0686	Identifique las vulnerabilidades ante posibles amenazas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios del servicio Amazon Elasticsearch tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	dynamodb-throughpu t-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/ write actividad que puede soportar cada tabla. DynamoDB utiliza esta informaci ón para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalm ente los parámetro s de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile información sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0706	Recopile informaci ón sobre las redes mediante técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas o análisis del tráfico).	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0777	Haga un perfil de los administradores de redes o sistemas y sus actividades.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0805	Informe sobre los eventos e intrusion es de red important es derivados de la inteligencia.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
T0877	Colabore con las unidades organizat ivas correspondientes para supervisar los derechos de acceso a la información del consumidor.	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0877	Colabore con las unidades organizativas correspondientes para supervisar los derechos de acceso a la información del consumidor.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0935	Realice una evaluación de los riesgos de seguridad de la información.	annual-risk-assessment-performed (verificación de procesos)	Realice una evaluación anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determinar la probabilidad y el impacto de los riesgos y and/or vulnerabilidades identificados que afectan a una organización.
T0960	Supervise los cambios en un sistema y su entorno de operación.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultaneidad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0960	Supervise los cambios en un sistema y su entorno de operación.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0960	Supervise los cambios en un sistema y su entorno de operación.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0960	Supervise los cambios en un sistema y su entorno de operación.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0960	Supervise los cambios en un sistema y su entorno de operación.	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0960	Supervise los cambios en un sistema y su entorno de operación.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0960	Supervise los cambios en un sistema y su entorno de operación.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada tabla. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
T0960	Supervise los cambios en un sistema y su entorno de operación.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0992	Determine cómo se utilizarán los resultados del monitoreo continuo en la autorización continua.	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de Administración de Claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: desencriptar,

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			kms:ReEncryptFrom) . Los valores reales deben reflejar las políticas de su organización.
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSymbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
T0993	Establezca herramientas y tecnologías de monitoreo continuo, procesos y procedimientos de control de acceso.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el NIST 800 181.

Prácticas operativas recomendadas para NIST 1800 25

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el NIST 1800-25 y las reglas de AWS Config administradas. Cada una AWS Config se aplica a un AWS recurso específico y se refiere a uno o más controles del NIST 1800-25. Un control NIST 1800-25 puede estar relacionado con varias reglas. AWS Config Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-1	Las vulnerabilidades de los activos se identifican y documentan	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-1	Las vulnerabilidades de los activos se identifican y documentan	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-1	Las vulnerabilidades de los activos se identifican y documentan	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-1	Las vulnerabilidades de los activos se identifican y documentan	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administr an, verifican, revocan y auditan las identidad es y credenciales para controlar los dispositivos, usuarios y procesos autorizad os	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administr an, verifican, revocan y auditan las identidad es y credenciales para controlar los dispositivos, usuarios y procesos autorizad os	iam-user-unused-cr edentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.
PR.AC-3	Se gestiona el acceso remoto.	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
PR.AC-3	Se gestiona el acceso remoto.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
PR.AC-3	Se gestiona el acceso remoto.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
PR.AC-3	Se gestiona el acceso remoto.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
PR.AC-3	Se gestiona el acceso remoto.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.AC-3	Se gestiona el acceso remoto.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.AC-3	Se gestiona el acceso remoto.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
PR.AC-3	Se gestiona el acceso remoto.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.AC-3	Se gestiona el acceso remoto.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegi o mínimo y separació n de funciones	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-1	Data-at-rest está protegido	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
PR.DS-1	Data-at-rest está protegido	sagemaker-notebook -instance-kms-conf igurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-1	Data-at-rest está protegido	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
PR.DS-1	Data-at-rest está protegido	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
PR.DS-1	Data-at-rest está protegido	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
PR.DS-1	Data-at-rest está protegido	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-1	Data-at-rest está protegido	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
PR.DS-2	Data-in-transit está protegido	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
PR.DS-2	Data-in-transit está protegido	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
PR.DS-2	Data-in-transit está protegido	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
PR.DS-2	Data-in-transit está protegido	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-6	Se utilizan mecanismos de control de integrida d para verificar la integridad del software, el firmware y la información	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-6	Se utilizan mecanismos de control de integrida d para verificar la integridad del software, el firmware y la información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información incorporando principio s de seguridad (por ejemplo, el concepto de mínima funcional idad)	account-part-of-or ganizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantiza r que las cuentas cumplan con las normas. La falta de gobernanza centraliz ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información que incorpora los principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima)	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información que incorpora los principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima)	ec2- -check managedinstance-as sociation-compliance-status	Use AWS Systems Manager Associati ons para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancia s administradas y le permite establecer líneas de referenci a de los niveles de parches del sistema operativo, las instalaci ones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima)	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima)	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información incorporando principio s de seguridad (por ejemplo, el concepto de mínima funcional idad)	redshift-cluster-m aintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configura ción preferida para su organización. En concreto, que tengan períodos de mantenimi ento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVers ionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-3	Existen procesos de control de los cambios de configuración	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
PR.IP-3	Existen procesos de control de los cambios de configuración	rds-instance-deletion-protection-activado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-9	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos y administrados.	response-plan-exists-maintained (Verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable. Contar con planes de respuesta actualizados y documentados formalmente puede ayudar a garantizar que el personal de respuesta comprenda los roles, responsabilidades y procesos que deben seguirse durante un incidente.
PR.IP-10	Se prueban los planes de respuesta y recuperación ante incidentes.	response-plan-tested (Verificación del proceso)	Asegúrese de que se prueben los planes de respuesta y recuperación ante incidentes. Esto puede ayudar a comprender si su plan será efectivo durante un incidente y si es necesario abordar alguna laguna o actualización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-12	Se ha desarrollado e implementado un plan de gestión de vulnerabilidades	vuln-management-plan-exists (Verificación del proceso)	Garantizar que se desarrolle e implemente un plan de administración de vulnerabilidades para disponer de procesos bien definidos para abordar las vulnerabilidades de su entorno. Esto puede incluir herramientas de administración de vulnerabilidades, cadencia de análisis del entorno, roles y responsabilidades.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-12	Se ha desarrollado e implementado un plan de gestión de vulnerabilidades	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-12	Se ha desarrollado e implementado un plan de gestión de vulnerabilidades	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-12	Se ha desarrollado e implementado un plan de gestión de vulnerabilidades	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.MA-2	Se aprueba, registra y realiza el mantenimiento remoto de los activos de la organización de manera que se evite el acceso no autorizado	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.MA-2	Se aprueba, registra y realiza el mantenimiento remoto de los activos de la organización de manera que se evite el acceso no autorizado	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Las redes de comunicaciones y control están protegidas	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorea r la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante el uso de fuentes de inteligen cia sobre amenazas. Estas incluyen listas de datos malicioso s IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
PR.PT-3	Se ha incorpora do el principio de mínima funcional idad al configurar los sistemas para que proporcio nen únicamente las capacidades esenciales	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
PR.PT-4	Las redes de comunicaciones y control están protegidas	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
PR.PT-4	Las redes de comunicaciones y control están protegidas	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
PR.PT-4	Las redes de comunicaciones y control están protegidas	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
PR.PT-4	Las redes de comunicaciones y control están protegidas	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
PR.PT-4	Las redes de comunicaciones y control están protegidas	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.PT-4	Las redes de comunicaciones y control están protegidas	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.PT-4	Las redes de comunicaciones y control están protegidas	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	s3- -bloques periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
PR.PT-4	Las redes de comunicaciones y control están protegidas	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-8	Se realizan escaneos de vulnerabilidades.	vuln-scans-performed (Verificación del proceso)	Asegúrese de que los escaneos de vulnerabilidades se realicen de acuerdo con sus requisitos de cumplimiento. Su organización debe definir la cadencia del escaneo, las herramientas utilizadas y el uso de los resultados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.MI-3	Las vulnerabilidades recientemente identificadas se mitigan o documentan como riesgos aceptados.	vuln-mitigated-accepted (Verificación del proceso)	Asegúrese de que las vulnerabilidades recientemente identificadas se corrijan o documenten como riesgos aceptados. Servicios como AWS Security Hub, Amazon Guard Duty, Amazon Inspector y AWS Config pueden ayudar a identificar las vulnerabilidades de su entorno. Las vulnerabilidades deben remediarse o aceptarse como riesgos de acuerdo con los requisitos de cumplimiento de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.MI-3	Las vulnerabilidades recientemente identificadas se mitigan o documentan como riesgos aceptados	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el NIST 1800 25.

Prácticas operativas recomendadas para el NIST CSF

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante

reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el Marco de Ciberseguridad (CSF) del NIST y las reglas de AWS Config administradas. Cada AWS Config regla se aplica a un AWS recurso específico y se refiere a uno o más controles del CSF del NIST. Un control del NIST CSF puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
DE.AE-1	Se establece y gestiona una referencia de operaciones	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	de red y flujos de datos esperados para los usuarios y los sistemas		de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referenci a de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referenci a de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referenci a de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referenci a de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referenci a de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referenci a de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referenci a de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-1	Se establece y gestiona una referencia de operaciones de red y flujos de datos esperados para los usuarios y los sistemas	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-2	Los eventos detectados se analizan para comprender los objetivos y métodos de ataque	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-2	Los eventos detectados se analizan para comprender los objetivos y métodos de ataque	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-3	Los datos de los eventos se recopilan y correlacionan desde múltiples fuentes y sensores	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
DE.AE-4	Se determina el impacto de los eventos	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-4	Se determina el impacto de los eventos	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-4	Se determina el impacto de los eventos	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-4	Se determina el impacto de los eventos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-4	Se determina el impacto de los eventos	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-4	Se determina el impacto de los eventos	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-4	Se determina el impacto de los eventos	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.AE-4	Se determina el impacto de los eventos	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	s3- event-notifications-enabled	Las notificaciones de eventos de Amazon S3 pueden alertar al personal pertinente de cualquier modificación accidental o intencionada en los objetos de su bucket. Algunos ejemplos de alertas son: creación de un objeto nuevo, eliminación de objetos, restauración de objetos, objetos perdidos o replicados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-1	Se monitorea la red en busca de posibles eventos de ciberseguridad	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
DE.CM-3	Se monitorea la actividad del personal en busca de posibles eventos de ciberseguridad	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-3	Se monitorea la actividad del personal en busca de posibles eventos de ciberseguridad	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a las API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-3	Se monitorea la actividad del personal en busca de posibles eventos de ciberseguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-3	Se monitorea la actividad del personal en busca de posibles eventos de ciberseguridad	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-3	Se monitorea la actividad del personal en busca de posibles eventos de ciberseguridad	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-3	Se monitorea la actividad del personal en busca de posibles eventos de ciberseguridad	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-4	Se ha detectado un código malicioso	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-4	Se ha detectado un código malicioso	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-5	Se ha detectado un código móvil no autorizado	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibi lidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
DE.CM-5	Se ha detectado un código móvil no autorizado	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-5	Se ha detectado un código móvil no autorizado	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-5	Se ha detectado un código móvil no autorizado	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-5	Se ha detectado un código móvil no autorizado	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-5	Se ha detectado un código móvil no autorizado	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-6	Se monitorea la actividad del proveedor de servicios externo en busca de posibles eventos de ciberseguridad	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-6	Se monitorea la actividad del proveedor de servicios externo en busca de posibles eventos de ciberseguridad	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-6	Se monitorea la actividad del proveedor de servicios externo en busca de posibles eventos de ciberseguridad	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-6	Se monitorea la actividad del proveedor de servicios externo en busca de posibles eventos de ciberseguridad	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-6	Se monitorea la actividad del proveedor de servicios externo en busca de posibles eventos de ciberseguridad	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-6	Se monitorea la actividad del proveedor de servicios externo en busca de posibles eventos de ciberseguridad	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-7	Se monitorea el personal, las conexiones, los dispositivos y el software no autorizados	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
DE.CM-7	Se monitorea el personal, las conexiones, los dispositivos y el software no autorizados	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la información de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-7	Se monitorea el personal, las conexiones, los dispositivos y el software no autorizados	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-7	Se monitorea el personal, las conexiones, los dispositivos y el software no autorizados	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-7	Se monitorea el personal, las conexiones, los dispositivos y el software no autorizados	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-7	Se monitorea el personal, las conexiones, los dispositivos y el software no autorizados	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-7	Se monitorea el personal, las conexiones, los dispositivos y el software no autorizados	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-7	Se monitorea el personal, las conexiones, los dispositivos y el software no autorizados	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.CM-7	Se monitorea el personal, las conexiones, los dispositivos y el software no autorizados	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.DP-4	Se comunica la información de detección de eventos	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.DP-4	Se comunica la información de detección de eventos	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
DE.DP-4	Se comunica la información de detección de eventos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.DP-4	Se comunica la información de detección de eventos	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.DP-4	Se comunica la información de detección de eventos	s3- event-notification s-enabled	Las notificaciones de eventos de Amazon S3 pueden alertar al personal pertinente de cualquier modificac ión accidental o intencionada en los objetos de su bucket. Algunos ejemplos de alertas son: creación de un objeto nuevo, eliminación de objetos, restauración de objetos, objetos perdidos o replicados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.DP-4	Se comunica la información de detección de eventos	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.DP-4	Se comunica la información de detección de eventos	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
DE.DP-5	Los procesos de detección se mejoran continuamente	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-2	Se hace inventario de las plataformas y aplicaciones de software de la organización	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.
ID.AM-3	La comunicación y los flujos de datos de la organización están mapeados	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-3	La comunicación y los flujos de datos de la organización están mapeados	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-3	La comunicación y los flujos de datos de la organización están mapeados	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-3	La comunicación y los flujos de datos de la organización están mapeados	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-3	La comunicación y los flujos de datos de la organización están mapeados	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-3	La comunicación y los flujos de datos de la organización están mapeados	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.AM-3	La comunicación y los flujos de datos de la organización están mapeados	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
ID.BE-5	Se han estableci do los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativo s (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operacion es normales)	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.BE-5	Se han establecido los requisitos de resiliencia para facilitar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción o ataque, durante la recuperación o durante las operaciones normales)	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-1	Las vulnerabilidades de los activos se identifican y documentan	rds-automatic-minor-version-habilitada para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-1	Las vulnerabilidades de los activos se identifican y documentan	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-1	Las vulnerabilidades de los activos se identifican y documentan	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-1	Las vulnerabilidades de los activos se identifican y documentan	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-2	La inteligencia sobre ciberamenazas se recibe de foros y fuentes de intercambio de información	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-3	Se identifican y documentan las amenazas, tanto internas como externas	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-3	Se identifican y documentan las amenazas, tanto internas como externas	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
ID.RA-5	Las amenazas, las vulnerabilidades, las probabilidades y los impactos se utilizan para determinar el riesgo	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-5	Las amenazas, las vulnerabilidades, las probabilidades y los impactos se utilizan para determinar el riesgo	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-5	Las amenazas, las vulnerabilidades, las probabilidades y los impactos se utilizan para determinar el riesgo	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.RA-5	Las amenazas, las vulnerabilidades, las probabilidades y los impactos se utilizan para determinar el riesgo	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.SC-4	Se evalúa a los proveedores y socios externos de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen sus obligaciones contractuales.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
ID.SC-4	Se evalúa a los proveedores y socios externos de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen sus obligaciones contractuales.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.SC-4	Se evalúa a los proveedores y socios externos de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen sus obligaciones contractuales.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.SC-4	Se evalúa a los proveedores y socios externos de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen sus obligaciones contractuales.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administr an, verifican, revocan y auditan las identidad es y credenciales para controlar los dispositivos, usuarios y procesos autorizad os	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
PR.AC-1	Se emiten, administr an, verifican, revocan y auditan las identidad es y credenciales para controlar los dispositivos, usuarios y procesos autorizad os	ecs-task-definition- user-for-host-mode- check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administr an, verifican, revocan y auditan las identidad es y credenciales para controlar los dispositivos, usuarios y procesos autorizad os	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los dispositivos, usuarios y procesos autorizados	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-1	Se emiten, administr an, verifican, revocan y auditan las identidad es y credenciales para controlar los dispositivos, usuarios y procesos autorizad os	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	autoscaling-launch-config-public-ip-deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
PR.AC-3	Se gestiona el acceso remoto.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
PR.AC-3	Se gestiona el acceso remoto.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
PR.AC-3	Se gestiona el acceso remoto.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
PR.AC-3	Se gestiona el acceso remoto.	lambda-function-pu blic-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibi lidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.AC-3	Se gestiona el acceso remoto.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.AC-3	Se gestiona el acceso remoto.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
PR.AC-3	Se gestiona el acceso remoto.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-3	Se gestiona el acceso remoto.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegi o mínimo y separació n de funciones	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red)	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-6	Las identidades se comprueban y se vinculan a las credenciales; también se afirman en las interacciones	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-6	Las identidades se comprueban y se vinculan a las credenciales; también se afirman en las interacciones	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por el NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-7	Se autentican los usuarios, los dispositivos y otros activos (por ejemplo, de un solo factor o de varios factores) en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizativos)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS funda mentales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-7	Se autentican los usuarios, los dispositivos y otros activos (por ejemplo, de un solo factor o de varios factores) en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizativos)	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS . Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-7	Se autentican los usuarios, los dispositivos y otros activos (por ejemplo, de un solo factor o de varios factores) en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizativos)	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-7	Se autentican los usuarios, los dispositivos y otros activos (por ejemplo, de un solo factor o de varios factores) en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizativos)	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-7	Se autentican los usuarios, los dispositivos y otros activos (por ejemplo, de un solo factor o de varios factores) en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizativos)	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AT-1	Todos los usuarios están informados y capacitados	security-awareness -program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infraccio nes o incidentes de seguridad.
PR.DS-1	Data-at-rest está protegido	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-1	Data-at-rest está protegido	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-1	Data-at-rest está protegido	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.
PR.DS-1	Data-at-rest está protegido	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
PR.DS-1	Data-at-rest está protegido	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
PR.DS-1	Data-at-rest está protegido	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-1	Data-at-rest está protegido	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-1	Data-at-rest está protegido	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
PR.DS-2	Data-in-transit está protegido	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
PR.DS-2	Data-in-transit está protegido	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
PR.DS-2	Data-in-transit está protegido	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-2	Data-in-transit está protegido	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
PR.DS-2	Data-in-transit está protegido	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-3	Los activos se gestionan formalmente durante la retirada, las transferencias y la enajenación	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-3	Los activos se gestionan formalmente durante la retirada, las transferencias y la enajenación	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-3	Los activos se gestionan formalmente durante la retirada, las transferencias y la enajenación	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-4	Capacidad adecuada para garantizar que se mantenga la disponibilidad	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	autoscaling-launch-config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	dms-replication-not-public	Gestiona el acceso a la AWS nube asegurándote de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
PR.DS-5	Se han implementado protecciones contra las filtraciones de datos	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-6	Se utilizan mecanismos de control de integrida d para verificar la integridad del software, el firmware y la información	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-6	Se utilizan mecanismos de control de integrida d para verificar la integridad del software, el firmware y la información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-7	Los entornos de desarrollo y prueba están separados del entorno de producción	ec2- -administrador instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-7	Los entornos de desarrollo y prueba están separados del entorno de producción	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-7	Los entornos de desarrollo y prueba están separados del entorno de producción	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-7	Los entornos de desarrollo y prueba están separados del entorno de producción	ec-2 volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-7	Los entornos de desarrollo y prueba están separados del entorno de producción	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-7	Los entornos de desarrollo y prueba están separados del entorno de producción	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima)	account-part-of-or ganizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantiza r que las cuentas cumplan con las normas. La falta de gobernanza centraliz ada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información que incorpora los principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima)	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información que incorpora los principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima)	ec2- -check managedinstance-as sociation-compliance-status	Use AWS Systems Manager Associati ons para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancia s administradas y le permite establecer líneas de referenci a de los niveles de parches del sistema operativo, las instalaci ones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima)	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima)	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-1	Se crea y mantiene una configura ción básica de los sistemas de technolog y/industrial control de la información incorporando principio s de seguridad (por ejemplo, el concepto de mínima funcional idad)	redshift-cluster-m aintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configura ción preferida para su organización. En concreto, que tengan períodos de mantenimi ento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVers ionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-2	Se ha implementado un ciclo de vida de desarrollo del sistema para gestionar los sistemas	codebuild-project-envvar-awscred-marcar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-2	Se ha implementado un ciclo de vida de desarrollo del sistema para gestionar los sistemas	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS OAuth Utilízalos en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-2	Se ha implementado un ciclo de vida de desarrollo del sistema para gestionar los sistemas	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-3	Existen procesos de control de los cambios de configuración	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
PR.IP-3	Existen procesos de control de los cambios de configuración	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-4	Se realizan, mantienen y prueban copias de seguridad de la información	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-7	Se mejoran los procesos de protecció n	ebs-optimized-inst ance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon I/O operation s. This optimization provides the most efficient performan ce for your EBS volumes by minimizin g contention between Amazon EBS I/O EBS y otro tráfico de la instancia.
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-8	Se comparte la eficacia de las tecnologías de protección	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-12	Se ha desarrollado e implementado un plan de gestión de vulnerabilidades	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-12	Se ha desarrollado e implementado un plan de gestión de vulnerabilidades	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.IP-12	Se ha desarrollado e implementado un plan de gestión de vulnerabilidades	ec2- -comprobar managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.MA-2	Se aprueba, registra y realiza el mantenimiento remoto de los activos de la organización de manera que se evite el acceso no autorizado	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.MA-2	Se aprueba, registra y realiza el mantenimiento remoto de los activos de la organización de manera que se evite el acceso no autorizado	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Las redes de comunicaciones y control están protegidas	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorea r la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	api-gw-execution-logging-activado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-1	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
PR.PT-3	Se ha incorpora do el principio de mínima funcional idad al configurar los sistemas para que proporcio nen únicamente las capacidades esenciales	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
PR.PT-4	Las redes de comunicaciones y control están protegidas	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
PR.PT-4	Las redes de comunicaciones y control están protegidas	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
PR.PT-4	Las redes de comunicaciones y control están protegidas	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
PR.PT-4	Las redes de comunicaciones y control están protegidas	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
PR.PT-4	Las redes de comunicaciones y control están protegidas	lambda-function-pu blic-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurán dose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibi lidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.PT-4	Las redes de comunicaciones y control están protegidas	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.PT-4	Las redes de comunicaciones y control están protegidas	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
PR.PT-4	Las redes de comunicaciones y control están protegidas	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-4	Las redes de comunicaciones y control están protegidas	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
PR.PT-5	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-5	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
RC.RP-1	El plan de recuperac ión se ejecuta durante o después de un incidente de ciberseguridad	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.AN-2	Se entiende el impacto del incidente	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.MI-3	Las vulnerabilidades recientemente identificadas se mitigan o documentan como riesgos aceptados	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
RS.RP-1	Se ejecuta un plan de respuesta durante o después de un incidente	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el CSF del NIST.

Prácticas operativas recomendadas para el NIST Privacy Framework v1.0

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de asignación entre el Marco de Privacidad NIST y las reglas de AWS Config administradas. Cada AWS Config regla se aplica a un AWS recurso específico y se refiere a uno o más controles del marco de privacidad del NIST. Un control del marco de privacidad del NIST puede estar relacionado con varias AWS Config reglas. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P7	Se han establecido e instaurado mecanismos para transmitir los permisos de procesamiento y los valores de datos relacionados con los elementos de datos.	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CT.DM-P7	Se han establecido e instaurado mecanismos para transmitir los permisos de	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	procesamiento y los valores de datos relacionados con los elementos de datos.		certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
CT.DM-P7	Se han establecido e instaurado mecanismos para transmitir los permisos de procesamiento y los valores de datos relacionados con los elementos de datos.	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P7	Se han establecido e instaurado mecanismos para transmitir los permisos de procesamiento y los valores de datos relacionados con los elementos de datos.	opensearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P7	Se han establecido e instaurado mecanismos para transmitir los permisos de procesamiento y los valores de datos relacionados con los elementos de datos.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P7	Se han establecido e instaurado mecanismos para transmitir los permisos de procesamiento y los valores de datos relacionados con los elementos de datos.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
CT.DM-P7	Se han establecido e instaurado mecanismos para transmitir los permisos de procesamiento y los valores de datos relacionados con los elementos de datos.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P7	Se han establecido e instaurado mecanismos para transmitir los permisos de procesamiento y los valores de datos relacionados con los elementos de datos.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
CT.DM-P7	Se han establecido e instaurado mecanismos para transmitir los permisos de procesamiento y los valores de datos relacionados con los elementos de datos.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	audit-log-policy-e xists(Verificación del proceso)	Establezca y mantenga una política de administr ación de registros de auditoría que defina los requisito s de registro de su organización. Esto incluye, pero no se limita a, la revisión y la conservación de los registros de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automátic o de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibi lidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexione s o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	api-gw-execution-l ogging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	cloudtrail-enabled	AWS CloudTrai l puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	cloudwatch-alarm-a ction-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluació n. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	dynamodb-throughpu t-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/ write actividad que puede soportar cada mesa. DynamoDB utiliza esta informaci ón para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalm ente los parámetro s de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitad o. Con el registro de Amazon RDS, puede capturar eventos tales como conexione s, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	rds-enhanced-monit oring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorea r la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	wafv2-logging-enab led	Para facilitar el registro y la supervisi ón en su entorno, habilite el registro con AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la informaci ón sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearc h Service tengan los registros de errores habilitados y transmiti dos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditoría s de seguridad y acceso, además de para diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitad os y transmitidos a Amazon CloudWatc h Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditoría s de seguridad y acceso, y pueden ayudar a diagnosti car problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	guardduty-non-arch ived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasifica ciones para determina r las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
CT.DM-P8	Los registros de auditoría y registro se determina n, documentan, implementan y revisan de acuerdo con la política e incorporando el principio de minimizac ión de datos.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
ID.DE-P2	Las partes del ecosistema de procesamiento de datos (por ejemplo, proveedores de servicios, clientes, socios, fabricantes de productos, desarrolladores de aplicaciones) se identifican, priorizan y evalúan mediante un proceso de evaluación de los riesgos de privacidad.	annual-risk-assessment-performed(Verificación del proceso)	Realice una evaluación anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determinar la probabilidad y el impacto de los riesgos y and/or vulnerabilidades identificados que afectan a una organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administr an, verifican, revocan y auditan las identidad es y credenciales para controlar los usuarios, procesos y dispositivos autorizad os	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administr ativos sobre cada una de las entidades principales.
PR.AC-P1	Se emiten, administr an, verifican, revocan y auditan las identidad es y credenciales para controlar los usuarios, procesos y dispositivos autorizad os	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P1	Se emiten, administran, verifican, revocan y auditan las identidades y credenciales para controlar los usuarios, procesos y dispositivos autorizados	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
PR.AC-P3	Se gestiona el acceso remoto.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
PR.AC-P3	Se gestiona el acceso remoto.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
PR.AC-P3	Se gestiona el acceso remoto.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.AC-P3	Se gestiona el acceso remoto.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.AC-P3	Se gestiona el acceso remoto.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	account-level-public-accesss3- -bloques-periódicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
PR.AC-P3	Se gestiona el acceso remoto.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
PR.AC-P3	Se gestiona el acceso remoto.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P3	Se gestiona el acceso remoto.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositor ios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las caracterí sticas de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegi o mínimo y separació n de funciones	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegi o mínimo y separació n de funciones	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegi o mínimo y separació n de funciones	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitadas las redes de host, pero el cliente no ha elegido los privilegios elevados.
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P4	Los permisos y autorizaciones de acceso se gestionan y se incorporan los principios de privilegio mínimo y separación de funciones	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red).	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red).	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red).	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red).	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red).	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red).	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red).	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentac ión de la red).	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P5	La integridad de la red está protegida (por ejemplo, mediante división o segmentación de la red).	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P6	Las personas y los dispositivos se comprueban, están sujetos a credencia les y se autentican en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizat ivos).	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P6	Las personas y los dispositivos se comprueban, están sujetos a credencia les y se autentican en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizat ivos).	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P6	Las personas y los dispositivos se comprueban, están sujetos a credencia les y se autentican en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizat ivos).	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P6	Las personas y los dispositivos se comprueban, están sujetos a credencia les y se autentican en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizat ivos).	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.AC-P6	Las personas y los dispositivos se comprueban, están sujetos a credencia les y se autentican en función del riesgo de la transacción (por ejemplo, los riesgos de seguridad y privacidad de las personas y otros riesgos organizat ivos).	root-account-mfa-e nabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protecció n a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	api-gw-cache-enabled-y cifrados	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-P1	Data-at-rest están protegidos.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
PR.DS-P1	Data-at-rest están protegidos.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-P1	Data-at-rest están protegidos.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
PR.DS-P1	Data-at-rest están protegidos.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-P1	Data-at-rest están protegidos.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	sagemaker-endpoint-configuration-kms-configurados por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	sagemaker-notebook-instance-kms-configurados por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-P1	Data-at-rest están protegidos.	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P1	Data-at-rest están protegidos.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
PR.DS-P2	Data-in-transit están protegidas.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P2	Data-in-transit están protegidos.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
PR.DS-P2	Data-in-transit están protegidos.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P2	Data-in-transit están protegidos.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
PR.DS-P2	Data-in-transit están protegidos.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que establezcas el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P4	Capacidad adecuada para garantizar que se mantenga la disponibilidad.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validació n de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credencia les AWS_ACCES S_KEY_ID de autenticación AWS_SECRE T_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild . No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposició n no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.DS-P5	Se han implementado protecciones contra las filtraciones de datos.	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
PR.DS-P6	Se utilizan mecanismos de control de integrida d para verificar la integridad del software, el firmware y la información.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.MA-P2	Se aprueba, registra y realiza el mantenimiento remoto de los activos de la organización de manera que se evite el acceso no autorizado.	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varias configuraciones. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.MA-P2	Se aprueba, registra y realiza el mantenimiento remoto de los activos de la organización de manera que se evite el acceso no autorizado.	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P1	Se crea y mantiene una configuración básica de tecnología de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima).	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las mejores prácticas de seguridad AWS recomendadas AWS CloudTrail, ya que comprueba la habilitación de varios ajustes. Estas incluyen el uso del cifrado de registros, la validación de registros y la habilitación AWS CloudTrail en varias regiones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P1	Se crea y mantiene una configuración básica de tecnología de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima).	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P1	Se crea y mantiene una configuración básica de tecnología de la información que incorpora principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P1	Se crea y mantiene una configuración básica de tecnología de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima).	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P1	Se crea y mantiene una configuración básica de tecnología de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima).	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P1	Se crea y mantiene una configuración básica de tecnología de la información que incorpora principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P1	Se crea y mantiene una configuración básica de tecnología de la información que incorpora principio s de seguridad (por ejemplo, el concepto de funcionalidad mínima).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P1	Se crea y mantiene una configuración básica de tecnología de la información que incorpora principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.
AT-1: PR.PO-P10	Se ha desarrollado e implementado un plan de gestión de vulnerabilidades	vuln-management-plan-exists(Verificación del proceso)	Garantizar que se desarrolle e implemente un plan de administración de vulnerabilidades para disponer de procesos bien definidos para abordar las vulnerabilidades de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P2	Existen procesos de control de los cambios de configuración establecidos y activos.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
PR.PO-P2	Existen procesos de control de los cambios de configuración establecidos y activos.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que establezcas el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P3	Se realizan, mantienen y prueban copias de seguridad de la información.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P7	Existen planes de respuesta (respuesta a incidentes y continuidad empresarial) y los planes de recuperación (recuperación ante incidentes y recuperación de desastres) establecidos, activos y administrados.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PO-P8	Se prueban los planes de respuesta y recuperación ante incidentes.	response-plan-tested(Verificación del proceso)	Asegúrese de que se prueben los planes de respuesta y recuperación ante incidentes. Esto puede ayudar a comprender si su plan será efectivo durante un incidente y si es necesario abordar alguna laguna o actualización.
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P2	Se ha incorporado el principio de mínima funcionalidad al configurar los sistemas para que proporcionen únicamente las capacidades esenciales.	redshift-enhanced-vpc-routing-habilitado	El enrutamiento de VPC mejorado fuerza que todo el tráfico de COPY y UNLOAD entre los repositorios de datos y de clúster pase por su Amazon VPC. A continuación, puede utilizar las características de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar los registros de flujo de la VPC para monitorear el tráfico de la red.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	s3- -bloques-periodicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	subnet-auto-assign-public-ip deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P3	Las redes de comunicaciones y control están protegidas.	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	elb-cross-zone-load-habilitado para el balanceo	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	backup-recovery-po int-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	backup-recovery-po int-manual-elimina ción-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperac ión. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implement ado mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercamb io en caliente) para cumplir con los requisitos de resilienc ia en situaciones normales y adversas.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
PR.PT-P4	Se han implemento mecanismos (por ejemplo, de prueba de fallos, equilibrio de carga o intercambio en caliente) para cumplir con los requisitos de resiliencia en situaciones normales y adversas.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

Plantilla

La plantilla está disponible en GitHub: Prácticas recomendadas operativas para la versión 1.0 del NIST Privacy Framework.

Prácticas operativas recomendadas para NYDFS 23

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes

de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre los requisitos de ciberseguridad del Departamento de Servicios Financieros (NYDFS) del Estado de Nueva York para las empresas de servicios financieros (23 NYCRR 500) y las reglas de Config gestionadas AWS . Cada AWS Config regla se aplica a un AWS recurso específico y se refiere a uno o más controles del NYDFS de EE. UU. Un control del NYDFS 23 NYCRR 500 puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.		de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	alb-http-drop-invalid-habilitado para encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidenc ialidad, integridad y disponibilidad de los sistemas de informaci ón de la entidad cubierta.	s3- bucket-default-loc k-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automáticamente cantidades equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	autoscaling-launch-config-public-ip deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	beanstalk-enhanced-health-reporting-activado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	s3- account-level-public-access -bloques-periodicos	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(a)	(a) Programa de ciberseguridad. Cada entidad cubierta mantendrá un programa de ciberseguridad diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información de la entidad cubierta.	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El IMDSv2 método utiliza controles basados en la sesión. Con IMDSv2, se pueden implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de cibersegu ridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimi entos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenad a en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de cibersegu ridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimi entos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenad a en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de cibersegu ridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimi entos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenad a en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de cibersegu ridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimi entos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenad a en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener información confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	[api-gw-associated-with-guerra](#)	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(2)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y estará diseñado para desempeñar las siguientes funciones básicas de ciberseguridad: (2) utilizar una infraestructura defensiva y aplicar políticas y procedimientos para proteger los sistemas de información de la entidad cubierta y la información no pública almacenada en esos sistemas de información contra el acceso, el uso o cualquier otro acto malintencionado no autorizados.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(3)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (3) detectar eventos de ciberseguridad.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	dynamodb-pitr-enab led	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantiza r que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	ebs-optimized-inst ance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/ O Esta optimizac ión proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/ O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeña r las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de cibersegu ridad y restaurar las operaciones y servicios normales.	backup-plan-min-fr equency-and-min-re tention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) y requiredF requencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
500.02(b)(5)	(b) El programa de ciberseguridad se basará en la evaluación de riesgos de la entidad cubierta y se diseñará para desempeñar las siguientes funciones básicas de ciberseguridad: (5) recuperarse de eventos de ciberseguridad y restaurar las operaciones y servicios normales.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.05	El programa de ciberseguridad de cada entidad cubierta incluirá el monitoreo y las pruebas, desarrollados de acuerdo con la evaluación de riesgos de la entidad cubierta, diseñados para evaluar la eficacia del programa de ciberseguridad de la entidad cubierta. El monitoreo y las pruebas deberán incluir un monitoreo continuo o pruebas de penetración y evaluaciones de vulnerabilidad periódicas. A falta de un monitoreo continuo efectivo o de otros sistemas para detectar de forma continua los cambios en los sistemas de información que puedan crear o indicar vulnerabilidades, las entidades cubiertas realizarán: (a) pruebas de	vuln-management-plan-exists (verificación del proceso)	Garantizar que se desarrolle e implemente un plan de administración de vulnerabilidades para disponer de procesos bien definidos para abordar las vulnerabilidades de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	penetración anuales de los sistemas de información de la entidad cubierta determinadas cada año en función de los riesgos identific ados relevantes de acuerdo con la evaluación de riesgos; y (b) evaluaciones de vulnerabilidad semestrales, incluidos cualquier escaneo o revisión sistemáti cos de los sistemas de información diseñados razonable mente para identific ar las vulnerabi lidades de cibersegu ridad conocidas públicamente en el los sistemas de informaci ón de la entidad cubierta basados en la evaluación del riesgo.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(b)	(b) Cada entidad cubierta mantendrá los registros requeridos por la sección 500.06(a)(1) de esta Parte durante al menos cinco años y mantendrá los registros requeridos por la sección 500.06(a)(2) de esta Parte durante al menos tres años.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.06(a)	(a) Cada entidad cubierta mantendrá de forma segura sistemas que, en la medida en que sea aplicable y sobre la base de su evaluación de riesgos: (1) estén diseñados para reconstruir las transacciones financieras importantes que respalden las operaciones y obligaciones normales de la entidad cubierta; e (2) incluyan registros de auditoría diseñados para detectar y responder a los eventos de ciberseguridad que tengan una probabilidad razonable de dañar materialmente cualquier parte importante de las operaciones normales de la entidad cubierta.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500,07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	ecs-task-definition-user-for-host-mode-check	Si la definición de una tarea tiene privilegios elevados, se debe a que el cliente ha optado específicamente por esa configura ción. Este control comprueba si hay una escalada inesperada de privilegios cuando una definición de tarea tiene habilitad as las redes de host, pero el cliente no ha elegido los privilegios elevados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500,07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	subnet-auto-assign-public-ip-deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500,07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
500,07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireLowercaseCharacters (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireSy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	s3- bucket-policy-grantee-check	Administre el acceso a la AWS nube habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados, principales de servicio, direcciones IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantáneas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube aseguránd ose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece seguro en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	s3- bucket-public-read-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegios de acceso de los usuarios a los sistemas de información que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.07	Como parte de su programa de ciberseguridad, sobre la base de la evaluación de riesgos de la entidad cubierta, cada entidad cubierta limitará los privilegi os de acceso de los usuarios a los sistemas de informaci ón que proporcionan acceso a información no pública y revisará periódicamente dichos privilegios de acceso.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.8(a)	(a) El programa de ciberseguridad de cada entidad cubierta incluirá procedimientos, directrices y estándares por escrito diseñados para garantizar el uso de prácticas de desarrollo seguras para las aplicaciones desarrolladas internamente que utilice la entidad cubierta, además de procedimientos para evaluar, valorar o comprobar la seguridad de las aplicaciones desarrolladas externamente que utilice la entidad cubierta en el contexto del entorno tecnológico de la entidad cubierta.	codebuild-project-envvar-awscred-comprobar	Asegúrese de que las credenciales AWS_ACCESS_KEY_ID de autenticación AWS_SECRET_ACCESS_KEY no existan en los entornos de proyectos de AWS Codebuild. No almacene estas variables en texto sin cifrar. El almacenamiento de estas variables en texto sin cifrar provoca una exposición no intencionada de los datos y un acceso no autorizado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.8(a)	(a) El programa de ciberseguridad de cada entidad cubierta incluirá procedimientos, directrices y estándares por escrito diseñados para garantizar el uso de prácticas de desarrollo seguras para las aplicaciones desarrolladas internamente que utilice la entidad cubierta, además de procedimientos para evaluar, valorar o comprobar la seguridad de las aplicaciones desarrolladas externamente que utilice la entidad cubierta en el contexto del entorno tecnológico de la entidad cubierta.	codebuild-project-source-repo-comprobar la URL	Asegúrese de que la URL del repositorio fuente GitHub o de Bitbucket no contenga tokens de acceso personales ni credenciales de inicio de sesión en los entornos de proyectos de Codebuild. AWS Úsalos OAuth en lugar de los tokens de acceso personales o las credenciales de inicio de sesión para conceder la autorización de acceso a los repositorios de Bitbucket GitHub .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.09	(a) Cada entidad cubierta realizará una evaluación periódica del riesgo de los sistemas de información de la entidad cubierta suficiente como para fundamentar el diseño del programa de ciberseguridad, según lo exige esta Parte. Dicha evaluación de riesgos se actualizará según sea razonable mente necesario para abordar los cambios en los sistemas de informaci ón, la informaci ón no pública o las operaciones comerciales de la entidad cubierta. La evaluación de riesgos de la entidad cubierta permitirá revisar los controles para responder a los avances tecnológi cos y la evolución de las amenazas, y tendrá en cuenta	annual-risk-assess ment-performed (verificación del proceso) >	Realice una evaluació n anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determina r la probabilidad y el impacto de los riesgos y and/or vulnerabi lidades identificados que afectan a una organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	los riesgos específicos de las operaciones comerciales de la entidad cubierta relacionados con la ciberseguridad, la información no pública recopilada o almacenada, los sistemas de información utilizados y la disponibilidad y eficacia de los controles para proteger la información y los sistemas de información no públicos.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.12	(a) Autenticación multifactor. Sobre la base de su evaluación de riesgos, cada entidad cubierta utilizará controles efectivos, que pueden incluir la autenticación multifactor o la autenticación basada en el riesgo, para protegerse contra el acceso no autorizado a información o sistemas de información no públicos. (b) La autenticación multifactor se utilizará para cualquier persona que acceda a las redes internas de la entidad cubierta desde una red externa, a menos que el CISO de la entidad cubierta haya aprobado por escrito el uso de controles de acceso razonablemente equivalentes o más seguros.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.12	(a) Autenticación multifactor. Sobre la base de su evaluación de riesgos, cada entidad cubierta utilizará controles efectivos, que pueden incluir la autenticación multifactor o la autenticación basada en el riesgo, para protegerse contra el acceso no autorizado a información o sistemas de información no públicos. (b) La autenticación multifactor se utilizará para cualquier persona que acceda a las redes internas de la entidad cubierta desde una red externa, a menos que el CISO de la entidad cubierta haya aprobado por escrito el uso de controles de acceso razonablemente equivalentes o más seguros.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.12	(a) Autenticación multifactor. Sobre la base de su evaluación de riesgos, cada entidad cubierta utilizará controles efectivos, que pueden incluir la autenticación multifactor o la autenticación basada en el riesgo, para protegerse contra el acceso no autorizado o a información o sistemas de información no públicos. (b) La autenticación multifactor se utilizará para cualquier persona que acceda a las redes internas de la entidad cubierta desde una red externa, a menos que el CISO de la entidad cubierta haya aprobado por escrito el uso de controles de acceso razonablemente equivalentes o más seguros.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.12	(a) Autenticación multifactor. Sobre la base de su evaluación de riesgos, cada entidad cubierta utilizará controles efectivos, que pueden incluir la autenticación multifactor o la autenticación basada en el riesgo, para protegerse contra el acceso no autorizado a información o sistemas de información no públicos. (b) La autenticación multifactor se utilizará para cualquier persona que acceda a las redes internas de la entidad cubierta desde una red externa, a menos que el CISO de la entidad cubierta haya aprobado por escrito el uso de controles de acceso razonablemente equivalentes o más seguros.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.12	(a) Autenticación multifactor. Sobre la base de su evaluación de riesgos, cada entidad cubierta utilizará controles efectivos, que pueden incluir la autenticación multifactor o la autenticación basada en el riesgo, para protegerse contra el acceso no autorizado o a información o sistemas de información no públicos. (b) La autenticación multifactor se utilizará para cualquier persona que acceda a las redes internas de la entidad cubierta desde una red externa, a menos que el CISO de la entidad cubierta haya aprobado por escrito el uso de controles de acceso razonablemente equivalentes o más seguros.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	cloudwatch-alarm-action-check	CloudWatch Las alarmas de Amazon alertan cuando una métrica supera el umbral durante un número específico de períodos de evaluación. La alarma realiza una o varias acciones según el valor de la métrica o expresión con respecto a un umbral durante varios períodos de tiempo. Esta regla requiere un valor para alarmActionRequired (Config Default: True), insufficientDataAction Obligatorio (Config Default: True) o okActionRequired (Config Default: False). El valor real debe reflejar las acciones de alarma de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro con AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a supervisar y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(a)	(a) implementar políticas, procedimientos y controles basados en el riesgo diseñados para monitorear la actividad de los usuarios autorizados y detectar el acceso no autorizado, el uso o la manipulación de información no pública por parte de dichos usuarios autorizados.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.14(b)	Como parte de su programa de ciberseguridad, cada entidad cubierta deberá: (b) ofrecer formación periódica sobre ciberseguridad a todo el personal, actualizada para reflejar los riesgos identificados por la entidad cubierta en su evaluación de riesgos.	security-awareness-program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infraccio nes o incidentes de seguridad.
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	api-gw-cache-enabl ed-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	alb-http-drop-invalid-habilitado para encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	elasticsearch-node-to-node-comprobación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitad o para su clúster de Amazon Redshift. Puesto que puede haber datos confidenc iales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.15(a)	(a) Como parte de su programa de ciberseguridad, sobre la base de su evaluación de riesgos, cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública en poder de o transmitida por la entidad cubierta, tanto en tránsito por redes externas como en reposo.	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
500.16	(a) Como parte de su programa de ciberseguridad, cada entidad cubierta establecerá un plan de respuesta a incidentes por escrito diseñado para responder rápidamente a cualquier evento de ciberseguridad que afecte sustancialmente a la confidencialidad, integrida d o disponibilidad de los sistemas de información de la entidad cubierta o al funcionamiento continuo de cualquier aspecto de los negocios u operaciones de la entidad cubierta.	response-plan-exists-maintained (verificación del proceso)	Asegúrese de que los planes de respuesta ante incidentes se establezcan, actualicen y distribuyan al personal responsable.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el NYDFS 23.

Prácticas operativas recomendadas para NZISM 3.8

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear comprobaciones de control de seguridad, operativas o de optimización de costos mediante reglas de AWS Config administradas o personalizadas y acciones correctivas de

AWS Config. Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de asignación entre el Manual de seguridad de la información (NZISM) de la Oficina de Seguridad de las Comunicaciones del Gobierno de Nueva Zelanda (GCSB) 2022-09, versión 3.8 y las reglas de AWS Managed Config. Cada regla de Config se aplica a un tipo de recurso específico de AWS que está relacionado con uno o más controles de NZISM. Un control del NZISM puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones. En las asignaciones solo se incluyen controles que representan la práctica recomendada o de línea de base para información clasificada como RESTRINGIDA o inferior.

Este ejemplo de plantilla de paquete de conformidad contiene asignaciones a los controles incluidos en el marco del NZISM, que es una parte integral del marco de requisitos de protección y seguridad (PSR) que establece las expectativas del Gobierno de Nueva Zelanda en lo que respecta a la gestión del personal, la información y la seguridad física.

El NZISM está licenciado bajo la licencia Creative Commons Attribution 4.0 de Nueva Zelanda, disponible en https://creativecommons.org/licenses/by/4.0/. La información sobre derechos de autor se encuentra en NZISM New Zealand Information Security Manual | Legal, Privacy, and Copyright.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1149	Seguridad del software, entornos operativos estándar, desarrollo de SOE de endurecimiento (14.1.8.C.01.)	ec2- -administrador instance-managed-by-systems	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, publicador y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1149	Seguridad del software, entornos operativos estándar, desarrollo de SOE de endurecimiento (14.1.8.C.01.)	ec2- -comprobar managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas de referencia de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1149	Seguridad del software, entornos operativos estándar, desarrollo de SOE de endurecimiento (14.1.8.C.01.)	ecs-containers-non privileged	Este control comprueba si el parámetro con privilegios de la definición de contenedor de las definiciones de tareas de Amazon ECS se establece como Verdadero. El control falla si este parámetro es igual a Verdadero . Este control solo evalúa la última revisión activa de una definición de tarea de Amazon ECS. Le recomenda mos que elimine los privilegios elevados de las definiciones de tareas de ECS. Cuando el parámetro de privilegio es True, el contenedor recibe privilegios elevados en la instancia de contenedor del host (similares a los del usuario raíz).

ID de control	Descripción del control	Regla de AWS Config	Directrices
1149	Seguridad del software, entornos operativos estándar, desarrollo de SOE de endurecimiento (14.1.8.C.01.)	ecs-containers-readonly-access	Este control comprueba si los contenedores de Amazon ECS están limitados al acceso de solo lectura a los sistemas de archivos raíz montados. Este control comprueba si el parámetro ReadonlyRootFilesystem de la definición de contenedor de las definiciones de tareas de Amazon ECS se establece como Falso. Este control solo evalúa la última revisión activa de una definición de tarea de Amazon ECS. Al habilitar esta opción, se reducen los vectores de ataque a la seguridad, ya que no se puede manipular ni escribir en el sistema de archivos de la instancia contenedora a menos que tenga permisos explícitos de lectura y escritura

ID de control	Descripción del control	Regla de AWS Config	Directrices
			en sus carpetas y directorios del sistema de archivos. Este control también se adhiere al principio de privilegio mínimo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1661	Seguridad del software, desarrollo de aplicaciones web, contenido de sitios web de agencia (14.5.6.C.01.)	cloudfront-default-root-object-configurado	Este control comprueba si una distribución de Amazon CloudFront está configurada para devolver un objeto específico que es el objeto raíz predeterminado. El control falla si la distribución de CloudFront no tiene configurado un objeto raíz predeterminado. A veces, un usuario puede solicitar la URL raíz de la distribución en lugar de un objeto de la distribución. Cuando esto sucede, especificar un objeto raíz predeterminado puede ayudarle a evitar la exposición del contenido de su distribución web. Esta regla debe aplicarse en la región us-east-1. Implemente con el parámetro de plantilla DeployEdgeRules = true

ID de control	Descripción del control	Regla de AWS Config	Directrices
1667	Seguridad del software, desarrollo de aplicaciones web, aplicaciones web (14.5.8.C.01.)	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida y compruebe que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration. El valor es 90 días.
1667	Seguridad del software, desarrollo de aplicaciones web, aplicaciones web (14.5.8.C.01.)	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1841	Control de acceso y contraseñas, identificación, autenticación y contraseñas, métodos de identificación y autenticación de usuarios del sistema (16.1.35.C.02.)	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1841	Control de acceso y contraseñas, identificación, autenticación y contraseñas, métodos de identificación y autenticación de usuarios del sistema (16.1.35.C.02.)	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios de IAM, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1841	Control de acceso y contraseñas, identificación, autenticación y contraseñas, métodos de identificación y autenticación de usuarios del sistema (16.1.35.C.02.)	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario con más privilegios en una cuenta de AWS. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1841	Control de acceso y contraseñas, identificación, autenticación y contraseñas, métodos de identificación y autenticación de usuarios del sistema (16.1.35.C.02.)	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario con más privilegios en una cuenta de AWS. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1847	Control de acceso y contraseñas, identificación, autenticación y contraseñas, protección de datos de autenticación en tránsito (16.1.37.C.01.)	alb-http-to-https-comprobación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1847	Control de acceso y contraseñas, identificación, autenticación y contraseñas, protección de datos de autenticación en tránsito (16.1.37.C.01.)	cloudfront-viewer-policy-https	Este control comprueba si una distribución de Amazon CloudFront requiere que los espectadores utilicen HTTPS directamente o si utiliza la redirección. El control falla si ViewerProtocolPolicy está configurado en allow-all para DefaultCacheBehavior o CacheBehaviors. Puede utilizar HTTPS (TLS) para ayudarle a evitar posibles ataques de tipo “intermediario”, de espionaje o de manipulación del tráfico de red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). Esta regla debe aplicarse en la región us-east-1. Implemente con el parámetro de plantilla DeployEdgeRules = true

ID de control	Descripción del control	Regla de AWS Config	Directrices
1847	Control de acceso y contraseñas, identificación, autenticación y contraseñas, protección de datos de autenticación en tránsito (16.1.37.C.01.)	elasticsearch-node-to-node-comprobación de cifrado	Este control comprueba si los dominios de Elasticsearch tienen habilitada la encriptación de nodo a nodo. Este control falla si el cifrado de nodo a nodo está deshabilitado en el dominio. HTTPS (TLS) puede utilizarse para ayudar a evitar posibles ataques de espionaje o de manipulación del tráfico de red con ataques de «persona en medio» o similares. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). Habilitar el cifrado de nodo a nodo para los dominios de Elasticsearch garantiza que las comunicaciones dentro del clúster se cifren en tránsito.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1847	Control de acceso y contraseñas, identificación, autenticación y contraseñas, protección de datos de autenticación en tránsito (16.1.37.C.01.)	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1847	Control de acceso y contraseñas, identificación, autenticación y contraseñas, protección de datos de autenticación en tránsito (16.1.37.C.01.)	opensearch-node-to-node-comprobación de cifrado	Este control comprueba si los dominios de OpenSearch tienen habilitado el cifrado de nodo a nodo. Este control falla si el cifrado de nodo a nodo está deshabilitado en el dominio. HTTPS (TLS) puede utilizarse para ayudar a evitar posibles ataques de espionaje o de manipulación del tráfico de red con ataques de «persona en medio» o similares. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). Habilitar el cifrado de nodo a nodo para los dominios de OpenSearch garantiza que las comunicaciones dentro del clúster se cifren en tránsito.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1858	Control de acceso y contraseñas, identificación, autenticación y contraseñas, política de selección de contraseñas (16.1.40.C.02.)	iam-password-policy	Puede utilizar HTTPS (TLS) para ayudarle a evitar posibles ataques de tipo “intermediario”, de espionaje o de manipulación del tráfico de red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
1893	Control de acceso y contraseñas, identificación, autenticación y contraseñas, suspensión de acceso (16.1.46.C.02.)	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla establece maxCredentialUsageAge en 30 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1946	Control de acceso y contraseñas, acceso de usuarios con privilegios, uso de cuentas con privilegios (16.3.5.C.02.)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, al restringir las políticas que incluyan Effect: Allow con Action: * sobre Resource: *. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1946	Control de acceso y contraseñas, acceso de usuarios con privilegios, uso de cuentas con privilegi os (16.3.5.C.02.)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de AWS basadas en roles para ayudar a incorporar el principio de funcional idad mínima.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1998	Control de acceso y contraseñas, registro y auditoría de eventos, mantenimiento de registros de administración del sistema (16.6.6.C.02.)	cloud-trail-cloud-watch-registros habilitados	Debe configurar CloudTrail con Registros de CloudWatch para monitorizar los registros de seguimiento y recibir notificaciones cuando se produzca una actividad específica. Esta regla comprueba si los registros de seguimiento de AWS CloudTrail están configurados para enviar registros a Registros de Amazon CloudWatch.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1998	Control de acceso y contraseñas, registro y auditoría de eventos, mantenimiento de registros de administración del sistema (16.6.6.C.02.)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
1998	Control de acceso y contraseñas, registro y auditoría de eventos, mantenimiento de registros de administración del sistema (16.6.6.C.02.)	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos. La retención mínima es de 18 meses.
2013	Control de acceso y contraseñas, registro y auditoría de eventos, eventos adicionales para registrar (16.6.10.C.02.)	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2013	Control de acceso y contraseñas, registro y auditoría de eventos, eventos adicionales para registrar (16.6.10. C.02.)	cloudfront-accesslogs-enabled	Este control comprueba si el registro de acceso al servidor está habilitado o en las distribuciones de CloudFront. El control falla si el registro de acceso no está habilitado para una distribución. Los registros de acceso de CloudFront proporcionan información detallada sobre cada solicitud de usuario que CloudFront recibe. Cada registro contiene información como la fecha y la hora en que se recibió la solicitud, la dirección IP del espectador que realizó la solicitud, el origen de la solicitud y el número de puerto de la solicitud del espectador. Estos registros son útiles para aplicaciones como auditorías de seguridad y acceso y

ID de control	Descripción del control	Regla de AWS Config	Directrices
			para investigaciones forenses. Esta regla debe aplicarse en la región us-east-1 . Implemente con el parámetro de plantilla DeployEdgeRules = true
2013	Control de acceso y contraseñas, registro y auditoría de eventos, eventos adicionales para registrar (16.6.10. C.02.)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2013	Control de acceso y contraseñas, registro y auditoría de eventos, eventos adicionales para registrar (16.6.10. C.02.)	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2013	Control de acceso y contraseñas, registro y auditoría de eventos, eventos adicionales para registrar (16.6.10. C.02.)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2013	Control de acceso y contraseñas, registro y auditoría de eventos, eventos adicionales para registrar (16.6.10. C.02.)	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2022	Control de acceso y contraseñas, registro y auditoría de eventos, protección del registro de eventos (16.6.12. C.01.)	cloud-trail-log-file-habilitada para validación	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2022	Control de acceso y contraseñas, registro y auditoría de eventos, protección del registro de eventos (16.6.12.C.01.)	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.
2028	Control de acceso y contraseñas, registro y auditoría de eventos, archivos del registro de eventos (16.6.13.C.01.)	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencialmente maliciosos. La retención mínima es de 18 meses.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenciales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos. Hay una exención disponible para los entornos de preproducción.
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	ec-2 ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	elasticsearch-encrypted-at-rest	Este control comprueba si los dominios de Elasticsearch tienen habilitada la configuración de cifrado en reposo. La comprobación falla si el cifrado en reposo no está habilitado. Para obtener una capa adicional de seguridad para la información confidencial, debe configurar su dominio de Elasticsearch Service de tal manera que esta información se cifre en reposo. Al configurar el cifrado de los datos en reposo, AWS KMS almacena y administra las claves de cifrado. Para realizar el cifrado, AWS KMS utiliza el algoritmo Estándar de cifrado avanzado con claves de 256 bits (AES-256).

ID de control	Descripción del control	Regla de AWS Config	Directrices
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	encrypted-volumes	Como los datos confidenciales pueden existir y para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	opensearch-encrypted-at-rest	Este control comprueba si los dominios de OpenSearch tienen habilitado el cifrado en reposo. La comprobación falla si el cifrado en reposo no está habilitado. Para obtener una capa adicional de seguridad para la información confidencial, debe configurar su dominio de OpenSearch Service de tal manera que se cifren en reposo. Al configurar el cifrado de los datos en reposo, AWS KMS almacena y administra las claves de cifrado. Para realizar el cifrado, AWS KMS utiliza el algoritmo Estándar de cifrado avanzado con claves de 256 bits (AES-256).

ID de control	Descripción del control	Regla de AWS Config	Directrices
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2082	Criptografía, fundamentos criptográficos, reducción de requisitos de almacenamiento y transferencia física (17.1.53.C.04.)	s3- default-encryption-kms	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de S3. Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos. Para obtener más información sobre el proceso y la administración del cifrado, utilice las CMK administradas por el cliente del AWS Key Management Service (AWS KMS). Hay una exención disponible para los buckets que contienen información no confidencial, siempre que esté habilitado SSE.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2090	Criptografía, fundamentos criptográficos, protección de la información y los sistemas (17.1.55. C.02.)	alb-http-to-https-comprobación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2090	Criptografía, fundamentos criptográficos, protección de la información y los sistemas (17.1.55. C.02.)	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2090	Criptografía, fundamentos criptográficos, protección de la información y los sistemas (17.1.55. C.02.)	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2598	Criptografía, seguridad de la capa de transporte, uso de TLS (17.4.16.C.01.)	elb-custom-security-policy-comprobación de SSL	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes SSL de su ElasticLoadBalancer clásico utilicen una política de seguridad personalizada. Estas políticas pueden proporcionar varios algoritmos criptográficos de alta seguridad para ayudar a garantizar las comunicaciones de red cifradas entre los sistemas. Esta regla requiere que establezca una política de seguridad personalizada para sus oyentes SSL. La política de seguridad predeterminada es: Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2600	Criptografía, seguridad de la capa de transporte, uso de TLS (17.4.16.C.02.)	elb-custom-security-policy-comprobación de SSL	Para ayudar a proteger los datos en tránsito, asegúrese de que sus oyentes SSL de su ElasticLoadBalancer clásico utilicen una política de seguridad personalizada. Estas políticas pueden proporcionar varios algoritmos criptográficos de alta seguridad para ayudar a garantizar las comunicaciones de red cifradas entre los sistemas. Esta regla requiere que establezca una política de seguridad personalizada para sus oyentes SSL. La política de seguridad predeterminada es: Protocol-TLSv1.2, ECDHE-ECDSA-AES128-GCM-SHA256.

ID de control	Descripción del control	Regla de AWS Config	Directrices
2726	Criptografía, Secure Shell, acceso remoto automatizado (17.5.8.C.02.)	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3021	Criptografía, administración de claves y contenido de KMP (17.9.25.C.01.)	cmk-backing-key-rotation-habilitado	AWS KMS permite a los clientes rotar la clave de respaldo, que es el material de claves almacenado en AWS KMS y que está vinculado al ID de clave de la CMK. Es la clave de backup que se utiliza para realizar operaciones criptográficas como, por ejemplo, cifrado y descifrado. Actualmente, la rotación de claves automática retiene todas las claves de backup anteriores, por lo que el descifrado de los datos cifrados se puede realizar de forma transparente. La rotación de claves de cifrado ayuda a reducir el impacto potencial de una clave en peligro porque los datos cifrados con una nueva clave no son accesibles con un clave anterior que se haya visto expuesta.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3205	Seguridad de redes, administración de redes, limitación del acceso a la red (18.1.13.C.02.)	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos. La lista de puertos de Internet autorizados es: solo 443

ID de control	Descripción del control	Regla de AWS Config	Directrices
3449	Seguridad de los productos, aplicación de parches y actualizaciones de productos, aplicación de parches a vulnerabilidades de los productos (12.4.4.C.02.)	ec2- -comprobar managedinstance-patch-compliance-status	Habilite la regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3449	Seguridad de los productos, aplicación de parches y actualizaciones de productos, aplicación de parches a vulnerabilidades de los productos (12.4.4.C.02.)	ecr-private-image-scanning-habilitado	Este control comprueba si un repositorio privado de ECR tiene configurado el análisis de imágenes. Este control falla si un repositorio privado de ECR no tiene configurado el análisis de imágenes. Tenga en cuenta que también debe configurar análisis al insertar para que cada repositorio pase este control. El escaneo de imágenes de ECR ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. ECR utiliza la base de datos de vulnerabilidades y exposiciones comunes (CVE) del proyecto Clair de código abierto y proporciona una lista de resultados de análisis. Al habilitar el análisis de imágenes

ID de control	Descripción del control	Regla de AWS Config	Directrices
			en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.
3449	Seguridad de los productos, aplicación de parches y actualizaciones de productos, aplicación de parches a vulnerabilidades de los productos (12.4.4.C.02.)	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla establece allowVersionUpgrade en TRUE.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3451	Seguridad de los productos, aplicación de parches y actualizaciones de productos, aplicación de parches a vulnerabilidades de los productos (12.4.4.C.04.)	ec2- -comprobar managedinstance-patch-compliance-status	Habilite la regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
3452	Seguridad de los productos, aplicación de parches y actualizaciones de productos, aplicación de parches a vulnerabilidades de los productos (12.4.4.C.05.)	ec2- -comprobar managedinstance-patch-compliance-status	Habilite la regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3452	Seguridad de los productos, aplicación de parches y actualizaciones de productos, aplicación de parches a vulnerabilidades de los productos (12.4.4.C.05.)	elastic-beanstalk-managed-updates-habilitado	Este control comprueba si las actualizaciones de plataforma gestionadas están habilitadas para el entorno de Elastic Beanstalk. Al habilitar las actualizaciones de plataforma administradas, se garantiza que se instalen las últimas correcciones, actualizaciones y funciones de la plataforma disponibles para el entorno. Mantenerse al día con la instalación de los parches es un paso importante para proteger los sistemas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3452	Seguridad de los productos, aplicación de parches y actualizaciones de productos, aplicación de parches a vulnerabilidades de los productos (12.4.4.C.05.)	rds-automatic-minor-version-habilitado para la actualización	Este control comprueba si las actualizaciones automáticas de las versiones secundarias están habilitadas para la instancia de base de datos de RDS. Al habilitar las actualizaciones automáticas de las versiones secundarias, se garantiza que se instalen las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS). Estas actualizaciones pueden incluir parches de seguridad y correcciones de errores. Mantenerse al día con la instalación de los parches es un paso importante para proteger los sistemas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3453	Seguridad de los productos, aplicación de parches y actualizaciones de los productos, reparación de las vulnerabilidades de los productos (12.4.4.C.06.)	ec2- -comprobar managedinstance-patch-compliance-status	Habilite la regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias de Amazon EC2 cumplen los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3453	Seguridad de los productos, aplicación de parches y actualizaciones de los productos, reparación de las vulnerabilidades de los productos (12.4.4.C.06.)	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla establece allowVersionUpgrade en TRUE.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicaciones web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno. Hay una exención disponible si el equilibrador de carga es el origen de una distribución de CloudFront con WAF habilitado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	api-gw-associated-with-guerra	Este control comprueba si una etapa de API Gateway utiliza una lista de control de acceso (ACL) web de AWS WAF. Este control falla si una ACL web regional de AWS WAF no está asociada a una etapa de la API de REST Gateway. AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las API de ataques. Le permite configura r una web ACL, que son un conjunto de reglas que permiten, bloquean o cuentan solicitudes web en función de las reglas y condicion es de seguridad web personalizables que defina. Asegúrese de que la etapa de API Gateway esté asociada a una ACL web de AWS

ID de control	Descripción del control	Regla de AWS Config	Directrices
			WAF para ayudar a protegerla de ataques malicioso s. Hay una exención disponible si la API Gateway es el origen de una distribución de CloudFront con WAF habilitado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	cloudfront-associated-with-waf	Este control comprueba si las distribuciones de CloudFront están asociadas a las ACL web de AWS WAF o AWS WAFv2. El control falla si la distribución no está asociada a una ACL web. AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las API de ataques. Le permite configurar un conjunto de reglas denominadas lista de control de acceso web (Web ACL) que permiten, bloquean o cuentan solicitud es web en función de las reglas y condicion es de seguridad web personalizables que defina. Asegúrese de que su distribución de CloudFront esté asociada a una ACL web de AWS WAF para protegerla de

ID de control	Descripción del control	Regla de AWS Config	Directrices
			ataques malicioso s. Esta regla debe aplicarse en la región us-east-1. Implement e con el parámetro de plantilla DeployEdg eRules = true
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicaci ón de DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El método IMDSv2 utiliza controles basados en sesiones. IMDSv2 permite implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	ec-2 instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Amazon VPC para gestionar correctamente el acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	elasticsearch-in-vpc-only	Este control comprueba si los dominios de Elasticsearch están en una VPC. No evalúa la configuración de direccionamiento de subred de VPC para determinar el acceso público. Debe asegurarse de que los dominios de Elasticsearch no están asociados a subredes públicas. Los dominios de Elasticsearch implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la red privada de AWS, sin necesidad de atravesar la Internet pública. Esta configuración aumenta la posición de seguridad al limitar el acceso a los datos en tránsito. Las VPC proporcionan una serie de controles de

ID de control	Descripción del control	Regla de AWS Config	Directrices
			red para proteger el acceso a los dominios de Elasticsearch, incluidas las ACL de red y los grupos de seguridad.
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	opensearch-in-vpc-only	Este control comprueba si los dominios de OpenSearch están en una VPC. No evalúa la configura ción de direccion amiento de subred de VPC para determina r el acceso público. Debe asegurarse de que los dominios de OpenSearch no están asociados a subredes públicas. Los dominios de OpenSearch implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la red privada de AWS, sin necesidad de atravesar la Internet pública. Esta configuración aumenta la posición de seguridad al limitar el acceso a los datos en tránsito. Las VPC proporcionan una serie de controles de

ID de control	Descripción del control	Regla de AWS Config	Directrices
			red para proteger el acceso a los dominios de OpenSearch, incluidas las ACL de red y los grupos de seguridad.
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla establece ignorePublicAcls en TRUE, blockPublicPolicy en TRUE, blockPublicAcls en TRUE y restrictPublicBuckets en TRUE.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcio nar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3562	Seguridad de puertas de enlace, puertas de enlace, configuración de puertas de enlace (19.1.12.C.01.)	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3623	Seguridad de puertas de enlace, puertas de enlace, zonas desmilitarizadas (19.1.14.C.02.)	elasticsearch-in-vpc-only	Este control comprueba si los dominios de Elasticsearch están en una VPC. No evalúa la configuración de direccionamiento de subred de VPC para determinar el acceso público. Debe asegurarse de que los dominios de Elasticsearch no están asociados a subredes públicas. Los dominios de Elasticsearch implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la red privada de AWS, sin necesidad de atravesar la Internet pública. Esta configuración aumenta la posición de seguridad al limitar el acceso a los datos en tránsito. Las VPC proporcionan una serie de controles de

ID de control	Descripción del control	Regla de AWS Config	Directrices
			red para proteger el acceso a los dominios de Elasticsearch, incluidas las ACL de red y los grupos de seguridad.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3623	Seguridad de puertas de enlace, puertas de enlace, zonas desmilitarizadas (19.1.14.C.02.)	opensearch-in-vpc-only	Este control comprueba si los dominios de OpenSearch están en una VPC. No evalúa la configura ción de direccion amiento de subred de VPC para determina r el acceso público. Debe asegurarse de que los dominios de OpenSearch no están asociados a subredes públicas. Los dominios de OpenSearch implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la red privada de AWS, sin necesidad de atravesar la Internet pública. Esta configuración aumenta la posición de seguridad al limitar el acceso a los datos en tránsito. Las VPC proporcionan una serie de controles de

ID de control	Descripción del control	Regla de AWS Config	Directrices
			red para proteger el acceso a los dominios de OpenSearch, incluidas las ACL de red y los grupos de seguridad.
3623	Seguridad de puertas de enlace, puertas de enlace, zonas desmilitarizadas (19.1.14.C.02.)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3623	Seguridad de puertas de enlace, puertas de enlace, zonas desmilitarizadas (19.1.14.C.02.)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3815	Seguridad de redes, detección y prevenció n de intrusiones, mantenimiento de IDS/IPS (18.4.9.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3857	Seguridad de redes, detección y prevención de intrusiones, configuración de IDS/IPS (18.4.11.C.01.)	guardduty-eks-protection-audit-habilitado	Este control comprueba si la supervisión de registros de auditoría de EKS en GuardDuty está activada. La supervisión de registros de auditoría de EKS en GuardDuty lo ayuda a detectar actividades potencialmente sospechosas en los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS). La supervisión de registros de auditoría de EKS utiliza los registros de auditoría de Kubernetes para capturar las actividades cronológicas de los usuarios, las aplicaciones que utilizan la API de Kubernetes y el plano de control.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3857	Seguridad de redes, detección y prevención de intrusiones, configuración de IDS/IPS (18.4.11.C.01.)	guardduty-eks-protection-runtime-habilitado	Este control comprueba si la supervisión en tiempo de ejecución de EKS en GuardDuty con administración automática de agentes está habilitada. La protección de EKS en Amazon GuardDuty proporciona una cobertura de detección de amenazas para ayudarlo a proteger los clústeres de Amazon EKS en su entorno de AWS. La supervisión en tiempo de ejecución de EKS utiliza los eventos de nivel de sistema operativo para ayudarlo a detectar posibles amenazas en los nodos y contenedores de EKS de sus clústeres de EKS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3857	Seguridad de redes, detección y prevención de intrusiones, configuración de IDS/IPS (18.4.11.C.01.)	guardduty-lambda-protection-enabled	Este control comprueba si la protección de Lambda en GuardDuty está activada. La protección de Lambda de GuardDuty ayuda a identificar posibles amenazas de seguridad cuando se invoca una función de AWS Lambda. Después de activar la protección de Lambda, GuardDuty comienza a supervisar los registros de actividad de red de Lambda asociados a las funciones de Lambda de su cuenta de AWS. Cuando una función de Lambda se invoca y GuardDuty identifica tráfico de red sospechos o que indica la presencia de un fragmento de código potencialmente malintencionado en su función de

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Lambda, GuardDuty genera un resultado.
3857	Seguridad de redes, detección y prevención de intrusiones, configuración de IDS/IPS (18.4.11.C.01.)	guardduty-s3-protection-enabled	Este control comprueba si la protección de S3 en GuardDuty está activada. La protección de S3 permite que GuardDuty monitorice las operaciones de la API de nivel de objeto para identificar los posibles riesgos de seguridad para los datos de los buckets de Amazon S3. GuardDuty supervisa las amenazas contra los recursos de S3 mediante el análisis de eventos de administración de AWS CloudTrail y eventos de datos de S3 CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3875	Seguridad de redes, detección y prevenció n de intrusiones, administración de eventos y correlación (18.4.12.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
3875	Seguridad de redes, detección y prevención de intrusiones, administración de eventos y correlación (18.4.12.C.01.)	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4333	Administración de datos, filtrado de contenido, validación de contenido (20.3.7.C.02.)	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicaciones web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4333	Administración de datos, filtrado de contenido, validación de contenido (20.3.7.C.02.)	api-gw-associated-with-guerra	Este control comprueba si una etapa de API Gateway utiliza una lista de control de acceso (ACL) web de AWS WAF. Este control falla si una ACL web regional de AWS WAF no está asociada a una etapa de la API de REST Gateway. AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las API de ataques. Le permite configurar una web ACL, que son un conjunto de reglas que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Asegúrese de que la etapa de API Gateway esté asociada a una ACL web de AWS

ID de control	Descripción del control	Regla de AWS Config	Directrices
			WAF para ayudar a protegerla de ataques malicioso s. Hay una exención disponible si la API Gateway es el origen de una distribución de CloudFront con WAF habilitado.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4441	Administración de datos, bases de datos, archivos de base de datos (20.4.4.C.02.)	elasticsearch-encrypted-at-rest	Este control comprueba si los dominios de Elasticsearch tienen habilitada la configuración de cifrado en reposo. La comprobación falla si el cifrado en reposo no está habilitado. Para obtener una capa adicional de seguridad para la información confidencial, debe configurar su dominio de Elasticsearch Service de tal manera que esta información se cifre en reposo. Al configurar el cifrado de los datos en reposo, AWS KMS almacena y administra las claves de cifrado. Para realizar el cifrado, AWS KMS utiliza el algoritmo Estándar de cifrado avanzado con claves de 256 bits (AES-256).

ID de control	Descripción del control	Regla de AWS Config	Directrices
4441	Administración de datos, bases de datos, archivos de base de datos (20.4.4.C.02.)	opensearch-encrypted-at-rest	Este control comprueba si los dominios de OpenSearch tienen habilitado el cifrado en reposo. La comprobación falla si el cifrado en reposo no está habilitado. Para obtener una capa adicional de seguridad para la información confidencial, debe configurar su dominio de OpenSearch Service de tal manera que se cifren en reposo. Al configurar el cifrado de los datos en reposo, AWS KMS almacena y administra las claves de cifrado. Para realizar el cifrado, AWS KMS utiliza el algoritmo Estándar de cifrado avanzado con claves de 256 bits (AES-256).

ID de control	Descripción del control	Regla de AWS Config	Directrices
4441	Administración de datos, bases de datos, archivos de base de datos (20.4.4.C.02.)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
4441	Administración de datos, bases de datos, archivos de base de datos (20.4.4.C.02.)	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4441	Administración de datos, bases de datos, archivos de base de datos (20.4.4.C.02.)	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4441	Administración de datos, bases de datos, archivos de base de datos (20.4.4.C.02.)	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4441	Administración de datos, bases de datos, archivos de base de datos (20.4.4.C.02.)	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla establece clusterDbEncrypted en TRUE y loggingEnabled en TRUE.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4445	Administración de datos, bases de datos, rendición de cuentas (20.4.5.C.02.)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4445	Administración de datos, bases de datos, rendición de cuentas (20.4.5.C.02.)	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla establece clusterDbEncrypted en TRUE y loggingEnabled en TRUE.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4829	Seguridad de los sistemas empresari ales, computación en la nube, disponibilidad del sistema (22.1.23. C.01.)	dynamodb-autoscali ng-enabled	El escalado automátic o de Amazon DynamoDB usa el servicio de escalado automático de aplicaciones de AWS para ajustar de manera automátic a la capacidad de rendimiento aprovisio nada en respuesta a los patrones de tráfico reales. Esto permite a una tabla o índice secundari o global increment ar su capacidad de lectura y escritura aprovisionada para gestionar incrementos repentinos del tráfico sin limitaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4829	Seguridad de los sistemas empresari ales, computación en la nube, disponibilidad del sistema (22.1.23. C.01.)	elb-cross-zone-loa d-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELB) para poder conservar la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4829	Seguridad de los sistemas empresari ales, computación en la nube, disponibilidad del sistema (22.1.23. C.01.)	rds-cluster-multi-az-habilitado	Amazon Aurora almacena copias de los datos en un clúster de bases de datos en varias zonas de disponibilidad en una única región de AWS. Aurora almacena estas copias independi entemente de si las instancias de base de datos en el clúster de base de datos abarcan varias zonas de disponibilidad. Cuando los datos se escriben en la instancia de base de datos principal , Aurora replica de forma síncrona los datos en zonas de disponibilidad a seis nodos de almacenam iento asociados con el volumen de clúster. Este enfoque proporcio na redundancia de datos, elimina los bloqueos de E/S y minimiza los picos de

ID de control	Descripción del control	Regla de AWS Config	Directrices
			latencia durante las copias de seguridad del sistema. Ejecutar una instancia de base de datos con alta disponibilidad puede mejorar la disponibilidad durante el mantenimiento de sistema planificado y ayuda a proteger las bases de datos contra los errores y las interrupciones de las zonas de disponibilidad. Esta regla comprueba si la replicación Multi-AZ está habilitada en los clústeres de Amazon Aurora administrados por Amazon RDS. Hay una exención disponible para los entornos de preproducción.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4829	Seguridad de los sistemas empresari ales, computación en la nube, disponibilidad del sistema (22.1.23. C.01.)	rds-multi-az-support	La compatibilidad con las zonas de disponibi lidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónic amente los datos en una instancia en espera en una zona de disponibi lidad diferente. Cada zona de disponibi lidad se ejecuta en su propia infraestr uctura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	Regla de AWS Config	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error. Hay una exención disponible para los entornos de preproducción.
4838	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.03.)	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen la informaci ón de la cuenta de AWS a la que ha accedido un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4838	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.03.)	ebs-snapshot-public-restorable-comprobar	Administre el acceso a la nube de AWS de manera que se garantice que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4838	Seguridad de los sistemas empresariales, computación en la nube, acceso no autorizado (22.1.24.C.03.)	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla establece ignorePublicAcls en TRUE, blockPublicPolicy en TRUE, blockPublicAcls en TRUE y restrictPublicBuckets en TRUE.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4838	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.03.)	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizad os acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
4838	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.03.)	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizad os acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresariales, computación en la nube, acceso no autorizado (22.1.24.C.04.)	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se cifran con una clave maestra de cliente (CMK) propiedad de AWS.
4839	Seguridad de los sistemas empresariales, computación en la nube, acceso no autorizado (22.1.24.C.04.)	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresariales, computación en la nube, acceso no autorizado (22.1.24.C.04.)	elasticsearch-encrypted-at-rest	Este control comprueba si los dominios de Elasticsearch tienen habilitada la configuración de cifrado en reposo. La comprobación falla si el cifrado en reposo no está habilitado. Para obtener una capa adicional de seguridad para la información confidencial, debe configurar su dominio de Elasticsearch Service de tal manera que esta información se cifre en reposo. Al configurar el cifrado de los datos en reposo, AWS KMS almacena y administra las claves de cifrado. Para realizar el cifrado, AWS KMS utiliza el algoritmo Estándar de cifrado avanzado con claves de 256 bits (AES-256).

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	elasticsearch-node-to-node-comprobación de cifrado	Este control comprueba si los dominios de Elasticse arch tienen habilitad a la encriptación de nodo a nodo. Este control falla si el cifrado de nodo a nodo está deshabili tado en el dominio. HTTPS (TLS) puede utilizarse para ayudar a evitar posibles ataques de espionaje o de manipulación del tráfico de red con ataques de «persona en medio» o similares . Solo se deben permitir las conexione s cifradas a través de HTTPS (TLS). Habilitar el cifrado de nodo a nodo para los dominios de Elasticse arch garantiza que las comunicaciones dentro del clúster se cifren en tránsito.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELB) estén configurados con oyentes SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	encrypted-volumes	Como los datos confidenciales pueden existir y para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresariales, computación en la nube, acceso no autorizado (22.1.24.C.04.)	opensearch-encrypted-at-rest	Este control comprueba si los dominios de OpenSearch tienen habilitado el cifrado en reposo. La comprobación falla si el cifrado en reposo no está habilitado. Para obtener una capa adicional de seguridad para la información confidencial, debe configurar su dominio de OpenSearch Service de tal manera que se cifren en reposo. Al configurar el cifrado de los datos en reposo, AWS KMS almacena y administra las claves de cifrado. Para realizar el cifrado, AWS KMS utiliza el algoritmo Estándar de cifrado avanzado con claves de 256 bits (AES-256).

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	opensearch-node-to -node-comprobación de cifrado	Este control comprueba si los dominios de OpenSearch tienen habilitado el cifrado de nodo a nodo. Este control falla si el cifrado de nodo a nodo está deshabili tado en el dominio. HTTPS (TLS) puede utilizarse para ayudar a evitar posibles ataques de espionaje o de manipulación del tráfico de red con ataques de «persona en medio» o similares . Solo se deben permitir las conexione s cifradas a través de HTTPS (TLS). Habilitar el cifrado de nodo a nodo para los dominios de OpenSearch garantiza que las comunicaciones dentro del clúster se cifren en tránsito.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresariales, computación en la nube, acceso no autorizado (22.1.24.C.04.)	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
4839	Seguridad de los sistemas empresariales, computación en la nube, acceso no autorizado (22.1.24.C.04.)	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla establece clusterDbEncrypted en TRUE y loggingEn abled en TRUE.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran cifrado TLS/SSL para conectarse a los clientes SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el punto de conexión de SageMaker. Puesto que puede haber datos confidenc iales en reposo en el punto de conexión de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	sagemaker-notebook -instance-kms-conf igurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para el cuaderno de SageMaker. Puesto que puede haber datos confidenc iales en reposo en el cuaderno de SageMaker, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresariales, computación en la nube, acceso no autorizado (22.1.24.C.04.)	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para los secretos de AWS Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4839	Seguridad de los sistemas empresari ales, computación en la nube, acceso no autorizado (22.1.24. C.04.)	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos. Hay una exención disponible cuando los mensajes publicados en el tema no contienen datos confidenciales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específic os para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	dynamodb-in-backup-plan	Para facilitar los procesos de copia de seguridad de los datos, asegúrese de que sus tablas de Amazon DynamoDB formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Hay una exención disponibl e cuando se ha configurado una solución de recuperac ión compensatoria.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresariales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la recuperación a un momento dado esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	ebs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Hay una exención disponibl e cuando se ha configurado una solución de recuperac ión compensatoria.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	efs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administr ado con una solución de copia de seguridad basada en políticas. Esta solución simplific a la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Hay una exención disponibl e cuando se ha configurado una solución de recuperac ión compensatoria.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando se habilitan las copias de seguridad automátic as, Amazon ElastiCac he crea una copia de seguridad del clúster diariamente. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	rds-cluster-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon RDS tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibi lidad de sus aplicacio nes.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalment e administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad. Hay una exención disponibl e cuando se ha configurado una solución de recuperac ión compensatoria.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	rds-instance-deletion-protection-habilitado	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	redshift-backup-en abled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantán eas automatizadas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantán eas de ese clúster periódicamente. De manera predeterm inada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	Regla de AWS Config	Directrices
4849	Seguridad de sistemas empresari ales, computación en la nube, copia de seguridad, archivo de recuperación y permanencia de datos (22.1.26.C.01.)	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperar se fácilmente de acciones no deseadas del usuario y de errores de la aplicació n. Hay una exención disponible cuando solo se va a crear una única variante de un objeto o cuando se ha configurado una solución de recuperac ión compensatoria.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6843	Control de acceso y contraseñas, administración de acceso privilegiado, principio del privilegio mínimo (16.4.31. C.02.)	mfa-enabled-for-iam-acceso a la consola	MFA aporta seguridad adicional al requerir a los usuarios que proporcionen autenticación exclusiva de un mecanismo de MFA compatible con AWS, además de sus credenciales de inicio de sesión habituales cuando accedan a sitios web o servicios de AWS. Los mecanismos compatibles incluyen claves de seguridad U2F, dispositivos MFA virtuales o de hardware y códigos basados en SMS. La regla comprueba si está habilitada a la autenticación multifactor (MFA) de AWS para todos los usuarios de Identity and Access Management(IAM) de AWS que utilizan una contraseña de la consola. La regla se

ID de control	Descripción del control	Regla de AWS Config	Directrices
			cumple si MFA está habilitado.
6843	Control de acceso y contraseñas, administración de acceso privilegiado, principio del privilegio mínimo (16.4.31. C.02.)	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario con más privilegios en una cuenta de AWS. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6852	Control de acceso y contraseñas, administración de acceso privilegiado, suspensión y revocación de las credenciales de acceso privilegiado (16.4.33.C.01.)	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla establece maxCredentialUsageAge en 30 días.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6860	Control de acceso y contraseñas, administración de acceso privilegiado, monitorización y revisión (16.4.35. C.02.)	cloud-trail-cloud-watch-registros habilitados	Debe configura r CloudTrail con Registros de CloudWatch para monitorizar los registros de seguimiento y recibir notificaciones cuando se produzca una actividad específica. Esta regla comprueba si los registros de seguimiento de AWS CloudTrail están configurados para enviar registros a Registros de Amazon CloudWatch.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6860	Control de acceso y contraseñas, administración de acceso privilegiado, monitorización y revisión (16.4.35. C.02.)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6861	Control de acceso y contraseñas, administración de acceso privilegiado, monitorización y revisión (16.4.35. C.03.)	cloudtrail-security-trail-enabled	Esta regla ayuda a garantizar el uso de las prácticas de seguridad recomendadas de AWS para AWS CloudTrail, ya que comprueba la habilitación de varios ajustes, como el uso del cifrado de registros, la validación de registros y la activación de AWS CloudTrail en varias regiones.

ID de control	Descripción del control	Regla de AWS Config	Directrices
6953	Control de acceso y contraseñas, autenticación multifactor, arquitectura del sistema y controles de seguridad (16.7.34. C.02.)	mfa-enabled-for-iam-acceso a la consola	MFA aporta seguridad adicional al requerir a los usuarios que proporcionen autenticación exclusiva de un mecanismo de MFA compatible con AWS, además de sus credenciales de inicio de sesión habituales cuando accedan a sitios web o servicios de AWS. Los mecanismos compatibles incluyen claves de seguridad U2F, dispositivos MFA virtuales o de hardware y códigos basados en SMS. La regla comprueba si está habilitada a la autenticación multifactor (MFA) de AWS para todos los usuarios de Identity and Access Management(IAM) de AWS que utilizan una contraseña de la consola. La regla se

ID de control	Descripción del control	Regla de AWS Config	Directrices
			cumple si MFA está habilitado.
6953	Control de acceso y contraseñas, autenticación multifactor, arquitectura del sistema y controles de seguridad (16.7.34. C.02.)	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario con más privilegios en una cuenta de AWS. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7436	Seguridad en la nube pública, administr ación de identidades y control de acceso, nombre de usuario y contraseñas (23.3.19. C.01.)	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7436	Seguridad en la nube pública, administr ación de identidades y control de acceso, nombre de usuario y contraseñas (23.3.19. C.01.)	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protecció n además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios de IAM, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7436	Seguridad en la nube pública, administración de identidades y control de acceso, nombre de usuario y contraseñas (23.3.19.C.01.)	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario con más privilegios en una cuenta de AWS. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7436	Seguridad en la nube pública, administración de identidades y control de acceso, nombre de usuario y contraseñas (23.3.19.C.01.)	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario con más privilegios en una cuenta de AWS. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7437	Seguridad en la nube pública, administr ación de identidades y control de acceso, nombre de usuario y contraseñas (23.3.19. C.01.)	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios de IAM. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseñ a. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios de IAM.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7437	Seguridad en la nube pública, administr ación de identidades y control de acceso, nombre de usuario y contraseñas (23.3.19. C.01.)	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protecció n además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios de IAM, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7437	Seguridad en la nube pública, administración de identidades y control de acceso, nombre de usuario y contraseñas (23.3.19.C.01.)	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario con más privilegios en una cuenta de AWS. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7437	Seguridad en la nube pública, administración de identidades y control de acceso, nombre de usuario y contraseñas (23.3.19.C.01.)	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario con más privilegios en una cuenta de AWS. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para el usuario raíz, puede reducir los incidentes de las cuentas de AWS comprometidas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	alb-waf-enabled	Asegúrese de que AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Una WAF ayuda a proteger sus aplicaciones web o API frente a las vulnerabilidades comunes de la web. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10. C.01.)	api-gw-associated-with-guerra	Este control comprueba si una etapa de API Gateway utiliza una lista de control de acceso (ACL) web de AWS WAF. Este control falla si una ACL web regional de AWS WAF no está asociada a una etapa de la API de REST Gateway. AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las API de ataques. Le permite configura r una web ACL, que son un conjunto de reglas que permiten, bloquean o cuentan solicitudes web en función de las reglas y condicion es de seguridad web personalizables que defina. Asegúrese de que la etapa de API Gateway esté asociada a una ACL web de AWS

ID de control	Descripción del control	Regla de AWS Config	Directrices
			WAF para ayudar a protegerla de ataques malicioso s. Hay una exención disponible si la API Gateway es el origen de una distribución de CloudFront con WAF habilitado.
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10. C.01.)	dms-replication-not-public	Administre el acceso a la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las instancias de replicaci ón de DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El método IMDSv2 utiliza controles basados en sesiones. IMDSv2 permite implementar controles para restringir los cambios en los metadatos de la instancia.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10. C.01.)	ec-2 instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	ec-2 instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	Regla de AWS Config	Directrices
			Amazon VPC para gestionar correctamente el acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	elasticsearch-in-vpc-only	Este control comprueba si los dominios de Elasticsearch están en una VPC. No evalúa la configuración de direccionamiento de subred de VPC para determinar el acceso público. Debe asegurarse de que los dominios de Elasticsearch no están asociados a subredes públicas. Los dominios de Elasticsearch implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la red privada de AWS, sin necesidad de atravesar la Internet pública. Esta configuración aumenta la posición de seguridad al limitar el acceso a los datos en tránsito. Las VPC proporcionan una serie de controles de

ID de control	Descripción del control	Regla de AWS Config	Directrices
			red para proteger el acceso a los dominios de Elasticsearch, incluidas las ACL de red y los grupos de seguridad.
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	emr-master-no-public-IP	Gestione el acceso a la nube de AWS de manera que garantice que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10. C.01.)	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperad a y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10. C.01.)	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	opensearch-in-vpc-only	Este control comprueba si los dominios de OpenSearch están en una VPC. No evalúa la configuración de direccionamiento de subred de VPC para determinar el acceso público. Debe asegurarse de que los dominios de OpenSearch no están asociados a subredes públicas. Los dominios de OpenSearch implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la red privada de AWS, sin necesidad de atravesar la Internet pública. Esta configuración aumenta la posición de seguridad al limitar el acceso a los datos en tránsito. Las VPC proporcionan una serie de controles de

ID de control	Descripción del control	Regla de AWS Config	Directrices
			red para proteger el acceso a los dominios de OpenSearch, incluidas las ACL de red y los grupos de seguridad.
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10. C.01.)	s3- account-level-public-access -bloques-periódicos	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla establece ignorePublicAcls en TRUE, blockPublicPolicy en TRUE, blockPublicAcls en TRUE y restrictPublicBuckets en TRUE.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los blocs de notas de Amazon SageMaker no permitan el acceso directo a internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10.C.01.)	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7466	Seguridad en la nube pública, protección de datos en la nube pública, accesibilidad de los datos (23.4.10. C.01.)	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
7496	Seguridad en la nube pública, registro y alertas en la nube pública, requisitos de registro (23.5.11. C.01.)	api-gw-execution-l ogging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta informaci ón permite ver las actividades de los usuarios.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7496	Seguridad en la nube pública, registro y alertas en la nube pública, requisitos de registro (23.5.11. C.01.)	cloud-trail-log-file-habilitada para validación	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validación de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7496	Seguridad en la nube pública, registro y alertas en la nube pública, requisitos de registro (23.5.11.C.01.)	cloudfront-accesslogs-enabled	Este control comprueba si el registro de acceso al servidor está habilitado en las distribuciones de CloudFront. El control falla si el registro de acceso no está habilitado para una distribución. Los registros de acceso de CloudFront proporcionan información detallada sobre cada solicitud de usuario que CloudFront recibe. Cada registro contiene información como la fecha y la hora en que se recibió la solicitud, la dirección IP del espectador que realizó la solicitud, el origen de la solicitud y el número de puerto de la solicitud del espectador. Estos registros son útiles para aplicaciones como auditorías de seguridad y acceso y

ID de control	Descripción del control	Regla de AWS Config	Directrices
			para investigaciones forenses. Esta regla debe aplicarse en la región us-east-1.
7496	Seguridad en la nube pública, registro y alertas en la nube pública, requisitos de registro (23.5.11. C.01.)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7496	Seguridad en la nube pública, registro y alertas en la nube pública, requisitos de registro (23.5.11. C.01.)	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.
7496	Seguridad en la nube pública, registro y alertas en la nube pública, requisitos de registro (23.5.11. C.01.)	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcionan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7496	Seguridad en la nube pública, registro y alertas en la nube pública, requisitos de registro (23.5.11. C.01.)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	Regla de AWS Config	Directrices
7496	Seguridad en la nube pública, registro y alertas en la nube pública, requisitos de registro (23.5.11. C.01.)	wafv2-logging-enabled	Para facilitar el registro y el monitoreo de su entorno, habilite el registro de AWS WAF (V2) en las ACL web regionales y globales. El registro de AWS El registro de WAF proporciona información detallada sobre el tráfico que analiza su ACL web. En los registros se incluye la hora en la que AWS WAF ha recibido la solicitud de su recurso de AWS, información detallada sobre la solicitud y una acción para la regla con la que coincide cada solicitud.

Plantilla

La plantilla está disponible en GitHub: Operational Best Practices for NZISM.

Prácticas operativas recomendadas para el PCI DSS 3.2.1

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el

cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) 3.2.1 y las reglas de AWS Config administradas. Cada AWS Config regla se aplica a un AWS recurso específico y se refiere a uno o más controles del PCI DSS. Un control del PCI DSS puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	alb-desync-mode-check	Para ayudar a proteger las aplicaciones contra las vulnerabilidades de desincronización HTTP, asegurar que el modo de mitigación de desincronización HTTP esté habilitado en los equilibradores de carga de aplicación. Los problemas de desincronización de HTTP pueden provocar el contrabando de solicitudes y hacer que sus aplicaciones sean vulnerables al envenenamiento de las colas de solicitudes o de la caché. La mitigación de desincronización incluye

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			modos monitorea dos, defensivos y más estrictos. El modo defensivo es el modo predeterminado.
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	alb-http-drop-invalid-habilitado para el encabezado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	netfw-stateless-rule-group-no está vacío	Un grupo de reglas de AWS Network Firewall contiene reglas que definen cómo el firewall procesa el tráfico en la VPC. Un grupo de reglas sin estado vacío, cuando está presente en una política de firewall, no procesa el tráfico.
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3	Prohíba el acceso público directo entre Internet y cualquier componente del sistema en el entorno de datos del titular de la tarjeta.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	netfw-policy-rule-group-asociado	Una política AWS de Network Firewall define la forma en que su firewall supervisa y gestiona el tráfico en una Amazon VPC. Puede configurar grupos de reglas sin y con estado para filtrar los paquetes y los flujos de tráfico, y definir la administr ación del tráfico predeterminado.
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	netfw-stateless-rule-group-no está vacío	Un grupo de reglas de AWS Network Firewall contiene reglas que definen cómo el firewall procesa el tráfico en la VPC. Un grupo de reglas sin estado vacío, cuando está presente en una política de firewall, no procesa el tráfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	subnet-auto-assign-public-IP deshabilitada	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna, segregados de la DMZ y otras redes que no sean de confianza.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1	Cambie siempre los valores predeterm inados proporcio nados por el proveedor y elimine o deshabilite las cuentas predeterm inadas innecesar ias antes de instalar un sistema en la red. Esto se aplica a todas las contraseñ as predeterminadas, incluidas, entre otras, las utilizadas por los sistemas operativo s, el software que proporciona servicios de seguridad, las cuentas de aplicacio nes y sistemas, los terminales point-of-sale (POS), las aplicaciones de pago, las cadenas comunitarias del Protocolo simple de administración de redes (SNMP), etc.).	rds-cluster-default-admin-compruebe	Como los nombres de usuario predeterm inados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de los clústeres de bases de datos de Amazon Relational Database Service (Amazon RDS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1	Cambie siempre los valores predeterminados proporcionados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red. Esto se aplica a TODAS las contraseñas predeterminadas, incluidas, entre otras, las utilizadas por los sistemas operativos, el software que proporciona servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales point-of-sale (POS), las aplicaciones de pago, las cadenas comunitarias del Protocolo simple de administración de redes (SNMP), etc.	rds-instance-default-admin-compruebe	Como los nombres de usuario predeterminados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de las instancias de bases de datos de Amazon Relational Database Service (Amazon RDS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1	Cambie siempre los valores predeterminados proporcionados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red. Esto se aplica a TODAS las contraseñas predeterminadas, incluidas, entre otras, las utilizadas por los sistemas operativos, el software que proporciona servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales point-of-sale (POS), las aplicaciones de pago, las cadenas comunitarias del Protocolo simple de administración de redes (SNMP), etc.	redshift-default-admin-check	Como los nombres de usuario predeterminados son de dominio público, cambiarlos puede ayudar a reducir la superficie expuesta a ataques de los clústeres de Amazon Redshift.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1	Cambie siempre los valores predeterminados proporcionados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red. Esto se aplica a TODAS las contraseñas predeterminadas, incluidas, entre otras, las utilizadas por los sistemas operativos, el software que proporciona servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales point-of-sale (POS), las aplicaciones de pago, las cadenas comunitarias del Protocolo simple de administración de redes (SNMP), etc.).	redshift-default-db-name-compruebe	Los nombres predeterminados son de dominio público y deben cambiarse durante la configuración. Cambiar el nombre de base de datos predeterminado de su clúster de Amazon Redshift puede ayudar a reducir la superficie expuesta a ataques de su clúster de Redshift.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1	Cambie siempre los valores predeterminados proporcionados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red. Esto se aplica a TODAS las contraseñas predeterminadas, incluidas, entre otras, las utilizadas por los sistemas operativos, el software que proporciona servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales point-of-sale (POS), las aplicaciones de pago, las cadenas comunitarias del Protocolo simple de administración de redes (SNMP), etc.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.1	Cambie siempre los valores predeterminados proporcionados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red. Esto se aplica a TODAS las contraseñas predeterminadas, incluidas, entre otras, las utilizadas por los sistemas operativos, el software que proporciona servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales point-of-sale (POS), las aplicaciones de pago, las cadenas comunitarias del Protocolo simple de administración de redes (SNMP), etc.).	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas en la industria se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por el sector se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identific ar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas en la industria se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizad os para garantiza r que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomenda da de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven compromet idas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los componentes del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándares de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados por la industria pueden incluir, entre otras: • Centro de Seguridad de Internet (CIS) • Organización Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por la industria se incluyen, entre otras, las siguiente s: • El Centro de Seguridad de Internet (CIS) • la Organizac ión Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	autoscaling-launch -config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, pero no se limitan a: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	cloud-trail-cloud-watch-Habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por la industria se incluyen, entre otras, las siguiente s: • El Centro de Seguridad de Internet (CIS) • la Organizac ión Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos almacenad os, asegúrese de que sus registros estén cifrados. AWS CloudTrail

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de reforzamiento de sistemas aceptadas en la industria se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas en la industria se incluyen, entre otras: • El Centro de Seguridad de Internet (CIS) • la Organizac ión Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por la industria se incluyen, entre otras: • El Centro de Seguridad de Internet (CIS) • la Organizac ión Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	cmk-backing-key-ro tation-habilitado	Habilite la rotación de claves para garantiza r que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándare s de refuerzo de sistemas aceptados en la industria pueden incluir, pero no se limitan a: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, pero no se limitan a: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	ec2- instance-multiple-eni-check	Esta regla comprueba si las instancias de Amazon Elastic Compute Cloud (Amazon EC2) tienen varias. ENIs Tener varias ENIs puede provocar instancia s de doble host, es decir, instancias que tienen varias subredes. Esto puede añadir complejidad a la seguridad de la red e introducir rutas y accesos a la red no deseados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los componentes del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándares de protección de sistemas aceptados por el sector. Entre las fuentes de estándares de refuerzo de sistemas aceptados en el sector se incluyen, entre otras, las siguientes: Centro de Seguridad de Internet (CIS), Organización Internacional de Normalización (ISO), Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS), Instituto Nacional de Tecnología de Estándares (NIST).	managedinstance-association-compliance-statusec2- -check	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los componentes del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándares de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por la industria se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	managedinstance-patch-compliance-statusec2- -check	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los componentes del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándares de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas en el sector se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	security-group-attached-toec2- -eni-periodic	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, pero no se limitan a: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados por la industria pueden incluir, entre otras: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	iam-no-inline-policy-compruebe	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los componentes del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándares de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por la industria se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados por la industria pueden incluir, entre otras: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los componentes del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándares de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, pero no se limitan a: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Estándares (NIST).	iam-user-group-membership-compruebe	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por la industria se incluyen, entre otras, las siguiente s: • El Centro de Seguridad de Internet (CIS) • la Organizac ión Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	iam-user-no-policies-compruebe	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por la industria se incluyen, entre otras, las siguiente s: • El Centro de Seguridad de Internet (CIS) • la Organizac ión Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	iam-user-unused-cr edentials-compruebe	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comproban do las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específic o. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegi o mínimo. Esta regla requiere que establezcas un valor en la maxCreden tialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, entre otras: • El Centro de Seguridad de Internet (CIS) • la Organizac ión Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Estándares (NIST).	mfa-enabled-for-iam-acceso desde consola	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Managemen t (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protecció n además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenc iales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por el sector se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por la industria se incluyen, entre otras, las siguiente s: • El Centro de Seguridad de Internet (CIS) • la Organizac ión Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	root-account-hardw are-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protecció n además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidente s de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los componentes del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándares de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas en la industria se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas en la industria se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	account-level-public-accesss3- -blocks-p eriodic	Gestione el acceso a los recursos en la AWS nube aseguránd ose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictPublicBuck ets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, entre otras: • El Centro de Seguridad de Internet (CIS) • la Organizac ión Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Estándares (NIST).	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de cibersegu ridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud , la acción solicitad a, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, pero no se limitan a: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los componentes del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándares de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas por la industria se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de reforzami ento de sistemas aceptadas en la industria se incluyen, entre otras, las siguientes: Centro de Seguridad de Internet (CIS), Organizac ión Internacional de Normalización (ISO), Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS), Instituto Nacional de Tecnología de Normalización (NIST).	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, pero no se limitan a: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	Compatible con s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, pero no se limitan a: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Las fuentes de estándares de endurecimiento de sistemas aceptados en la industria pueden incluir, pero no se limitan a: • Centro de Seguridad de Internet (CIS) • Organizac ión Internacional de Normalización (ISO) • Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • Instituto Nacional de Tecnología de Estándares (NIST).	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2	Desarrolle estándares de configuración para todos los component es del sistema. Asegúrese de que estos estándares aborden todas las vulnerabilidades de seguridad conocidas y sean coherentes con los estándare s de protección de sistemas aceptados por el sector. Entre las fuentes de normas de refuerzo de sistemas aceptadas en la industria se incluyen, entre otras, las siguientes: • El Centro de Seguridad de Internet (CIS) • la Organización Internacional de Normalización (ISO) • el Instituto de SysAdmin Auditoría de Seguridad de Redes (SANS) • el Instituto Nacional de Tecnología de Normalización (NIST).	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	autoscaling-launch-config-public-ip deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicación del DMS. Las instancias de replicación de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	emr-master-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctamente el acceso.
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura en la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamie nto de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	s3- bucket-level-public-access -prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicament e los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.2	Habilite únicamente los servicios, protocolos, daemons, etc. necesarios para el funcionamiento del sistema.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.3	Implemente funciones de seguridad adicionales para todos los servicios, protocolos o daemons necesarios que se consideren inseguros.	alb-desync-mode-check	Para ayudar a proteger las aplicaciones contra las vulnerabilidades de desincronización HTTP, asegurar que el modo de mitigación de desincronización HTTP esté habilitado en los equilibradores de carga de aplicación. Los problemas de desincronización de HTTP pueden provocar el contrabando de solicitudes y hacer que sus aplicaciones sean vulnerables al envenenamiento de las colas de solicitudes o de la caché. La mitigación de desincronización incluye modos monitoreados, defensivos y más estrictos. El modo defensivo es el modo predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.3	Cifre todos los accesos administr ativos que no sean de consola mediante una criptografía sólida.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2.3	Cifre todos los accesos administr ativos que no sean de consola mediante una criptografía sólida.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.3	Cifre todos los accesos administr ativos que no sean de consola mediante una criptografía sólida.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
2.3	Cifre todos los accesos administr ativos que no sean de consola mediante una criptografía sólida.	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.3	Cifre todos los accesos administr ativos que no sean de consola mediante una criptografía sólida.	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.
2.4	Mantenga un inventari o de los componentes del sistema que están dentro del ámbito de PCI DSS.	ec2- -eni-periodic security-group-att ached-to	Esta regla garantiza que los grupos de seguridad estén asociados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o a una ENI. Esta regla ayuda a monitorear los grupos de seguridad no utilizados en el inventario y la administración de su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.4	Mantenga un inventario de los componentes del sistema que están dentro del ámbito de PCI DSS.	eip-attached	Esta regla garantiza que las IP elásticas asignadas a una Amazon Virtual Private Cloud (Amazon VPC) estén conectadas a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a interfaces de red elástica en uso. Esta regla ayuda a supervisar los elementos no utilizados EIPs en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.4	Mantenga un inventario de los componentes del sistema que están dentro del ámbito de PCI DSS.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.4	Mantenga un inventario de los componentes del sistema que están dentro del ámbito de PCI DSS.	vpc-network-acl-unused-comprobar	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1	Mantenga el almacenamiento de datos de los titulares de tarjetas al mínimo mediante la implementación de políticas, procedimientos y procesos de retención y eliminación de datos que incluyan al menos lo siguiente para todo el almacenamiento de datos del titular de la tarjeta (CHD): • Limitar la cantidad de almacenamiento de datos y el tiempo de retención a lo requerido por los requisitos legales, reglamentarios y and/or comerciales • Requisitos de retención específicos para los datos del titular de la tarjeta • Procesos para la eliminación segura de los datos cuando ya no se necesiten • Un proceso trimestral para identificar y	s3- lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	eliminar de forma segura los datos del titular de la tarjeta almacenados que superen la retención definida.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1	Mantenga el almacenamiento de datos de los titulares de tarjetas al mínimo mediante la implementación de políticas, procedimientos y procesos de retención y eliminación de datos que incluyan al menos lo siguiente para todo el almacenamiento de datos del titular de la tarjeta (CHD): • Limitar la cantidad de almacenamiento de datos y el tiempo de retención a lo requerido por los requisitos legales, reglamentarios y and/or comerciales • Requisitos de retención específicos para los datos del titular de la tarjeta • Procesos para la eliminación segura de los datos cuando ya no se necesiten • Un proceso trimestral para identificar y	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	eliminar de forma segura los datos del titular de la tarjeta almacenados que superen la retención definida.		default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1	Mantenga el almacenamiento de datos de los titulares de tarjetas al mínimo mediante la implementación de políticas, procedimientos y procesos de retención y eliminación de datos que incluyan al menos lo siguiente para todo el almacenamiento de datos del titular de la tarjeta (CHD): • Limitar la cantidad de almacenamiento de datos y el tiempo de retención a lo requerido por los requisitos legales, reglamentarios y and/or comerciales • Requisitos de retención específicos para los datos del titular de la tarjeta • Procesos para la eliminación segura de los datos cuando ya no se necesiten • Un proceso trimestral para identificar y	backup-recovery-point-minimum- control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	eliminar de forma segura los datos del titular de la tarjeta almacenados que superen la retención definida.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1	Mantenga el almacenamiento de datos de los titulares de tarjetas al mínimo mediante la implementación de políticas, procedimientos y procesos de retención y eliminación de datos que incluyan al menos lo siguiente para todo el almacenamiento de datos del titular de la tarjeta (CHD): • Limitar la cantidad de almacenamiento de datos y el tiempo de retención a lo requerido por los requisitos legales, reglamentarios y and/or comerciales • Requisitos de retención específicos para los datos del titular de la tarjeta • Procesos para la eliminación segura de los datos cuando ya no se necesiten • Un proceso trimestral para identificar y	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	eliminar de forma segura los datos del titular de la tarjeta almacenados que superen la retención definida.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en sus AWS CloudTrail registros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	efs-encrypted-check	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	rds-snapshot-encry pted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	sagemaker-notebook -instance-kms-conf igurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.4	Haga que el PAN sea ilegible en cualquier lugar donde esté almacenado (incluidos los soportes digitales portátiles, los medios de copia de seguridad y los registros) mediante cualquiera de los siguientes enfoques: • Hashes unidirecc ionales basados en una criptografía sólida (el hash debe ser de todo el PAN) • Truncamiento (el hash no se puede utilizar para reemplazar el segmento truncado del PAN) • Indexar tokens y cuadernos (los cuadernos deben almacenarse de forma segura) • Criptografía sólida con procesos y procedimientos de administración de claves asociados . Nota: Reconstru ir los datos de PAN originales es un esfuerzo relativam	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	ente trivial para una persona malintenc ionada si tiene acceso a la versión truncada y codificada de un PAN. Cuando en el entorno de una entidad haya versiones con hash y truncadas del mismo PAN, deben existir controles adicional es para garantiza r que las versiones con hash y truncadas no puedan correlaci onarse para reconstru ir el PAN original.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.2	Restrinja el acceso a las claves criptográficas al menor número de custodios necesario.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.2	Restrinja el acceso a las claves criptográficas al menor número de custodios necesario.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.3	Guarde las claves secretas y privadas utilizadas para los datos del encrypt/decrypt titular de la tarjeta en todo momento en una (o más) de las siguientes formas: • Cifradas con una clave de cifrado que sea al menos tan segura como la clave de cifrado de datos y que se almacene por separado de la clave de cifrado de datos • Dentro de un dispositivo criptográfico seguro (como un módulo de seguridad de hardware (host) (HSM) o un point-of-interaction dispositivo aprobado por PTS) • Como mínimo dos componentes clave completos o acciones clave, de acuerdo con un método aceptado en la industria Nota: No es necesario que las claves públicas se	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	almacenen en una de estas formularios.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.3	Guarde las claves secretas y privadas utilizadas para los datos del encrypt/decrypt titular de la tarjeta en todo momento en una (o más) de las siguientes formas: • Cifradas con una clave de cifrado que sea al menos tan segura como la clave de cifrado de datos y que se almacene por separado de la clave de cifrado de datos • Dentro de un dispositivo criptográfico seguro (como un módulo de seguridad de hardware (host) (HSM) o un point-of-interaction dispositivo aprobado por PTS) • Como mínimo dos componentes clave completos o acciones clave, de acuerdo con un método aceptado en la industria Nota: No es necesario que las claves públicas se	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	almacenen en una de estas formularios.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.3	Guarde las claves secretas y privadas utilizadas para los datos del encrypt/decrypt titular de la tarjeta en todo momento en una (o más) de las siguientes formas: • Cifradas con una clave de cifrado que sea al menos tan segura como la clave de cifrado de datos y que se almacene por separado de la clave de cifrado de datos • Dentro de un dispositivo criptográfico seguro (como un módulo de seguridad de hardware (host) (HSM) o un point-of-interaction dispositivo aprobado por PTS) • Como mínimo dos componentes clave completos o acciones clave, de acuerdo con un método aceptado en la industria Nota: No es necesario que las claves públicas se	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	almacenen en una de estas formularios.		
3.6.4	Los cambios de clave criptográfica de las claves que han llegado al final de su criptoperíodo (por ejemplo, una vez transcurrido un período de tiempo definido, and/or después de que una clave determina da haya generado cierta cantidad de texto cifrado), según lo definido por el proveedor de la aplicación correspon diente o el propietar io de la clave, y en función de las mejores prácticas y directrices del sector (por ejemplo, la publicación especial 800-57 del NIST).	cmk-backing-key-ro tation-activado	Habilite la rotación de claves para garantiza r que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.5	La retirada o la sustitución (por ejemplo, archivando, destruyendo o and/or revocando) de las claves, según se considere necesario, cuando la integridad de la clave se haya debilitado (por ejemplo, cuando un empleado se vaya por el conocimiento de un componente clave en texto claro), o cuando se sospeche que las claves están en peligro. Nota: Si es necesario conservar las claves criptográficas retiradas o sustituidas, estas claves deben archivarse de forma segura (por ejemplo, mediante una clave de cifrado). Las claves criptográficas archivadas solo deben usarse con fines específicos. decryption/verification	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.7	Prevención de la sustitución no autorizada de claves criptográficas.	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que AWS ACM emita los certificados X509. Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	alb-http-to-https-verificación de redirección	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitudes HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.1	Utilice protocolos de seguridad y criptografía rigurosos para proteger los datos confidenciales de los titulares de tarjetas durante su transmisión a través de redes públicas y abiertas, incluidos los siguientes: • Solo se aceptan claves y certificados fiables. • El protocolo en uso solo admite versiones o configuraciones seguras. • La potencia de cifrado es adecuada para la metodología de cifrado utilizada. Los ejemplos de redes públicas y abiertas incluyen, pero no se limitan a: • Internet • Tecnologías inalámbricas, incluidas la 802.11 y el Bluetooth • Tecnologías de telefonía celular, por ejemplo, el Sistema Global de Comunicaciones Móviles (GSM), el acceso múltiple por	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	división de códigos (CDMA) • Servicio General de Radio por Paquetes (GPRS) • Comunicaciones por satélite		
6.2	Asegúrese de que todos los component es del sistema y el software estén protegidos contra vulnerabilidades conocidas mediante la instalación de parches de seguridad proporcionados por el proveedor. Instale parches de seguridad críticos en el plazo de un mes a partir del lanzamiento. Nota: Los parches de seguridad críticos deben identific arse de acuerdo con el proceso de clasificación de riesgos definido en el requisito 6.1.	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionad as para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correccio nes, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomenda da para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.2	Asegúrese de que todos los component es del sistema y el software estén protegidos contra vulnerabilidades conocidas mediante la instalación de parches de seguridad proporcionados por el proveedor. Instale parches de seguridad críticos en el plazo de un mes a partir del lanzamiento. Nota: Los parches de seguridad críticos deben identific arse de acuerdo con el proceso de clasificación de riesgos definido en el requisito 6.1.	ec2- -check managedinstance-as sociation-compliance-status	Use AWS Systems Manager Associati ons para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancia s administradas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.2	Asegúrese de que todos los componentes del sistema y el software estén protegidos contra vulnerabilidades conocidas mediante la instalación de parches de seguridad proporcionados por el proveedor. Instale parches de seguridad críticos en el plazo de un mes a partir del lanzamiento. Nota: Los parches de seguridad críticos deben identificarse de acuerdo con el proceso de clasificación de riesgos definido en el requisito 6.1.	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.2	Asegúrese de que todos los component es del sistema y el software estén protegidos contra vulnerabilidades conocidas mediante la instalación de parches de seguridad proporcionados por el proveedor. Instale parches de seguridad críticos en el plazo de un mes a partir del lanzamiento. Nota: Los parches de seguridad críticos deben identific arse de acuerdo con el proceso de clasificación de riesgos definido en el requisito 6.1.	ecs-fargate-latest-platform-versión	Las actualizaciones y los parches de seguridad se implementan automáticamente para sus tareas de AWS Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma AWS Fargate, aplique AWS parches a la versión de la plataforma. Para facilitar la administr ación de parches de las tareas de Amazon Elastic Container Service (ECS) que ejecutan AWS Fargate, actualice las tareas independi entes de sus servicios para usar la versión de plataforma más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.2	Asegúrese de que todos los component es del sistema y el software estén protegidos contra vulnerabilidades conocidas mediante la instalación de parches de seguridad proporcionados por el proveedor. Instale parches de seguridad críticos en el plazo de un mes a partir del lanzamiento. Nota: Los parches de seguridad críticos deben identific arse de acuerdo con el proceso de clasificación de riesgos definido en el requisito 6.1.	rds-automatic-mino r-version-habilitada para la actualización	Habilite las actualiza ciones automátic as de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundari as del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correccio nes de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.2	Asegúrese de que todos los component es del sistema y el software estén protegidos contra vulnerabilidades conocidas mediante la instalación de parches de seguridad proporcionados por el proveedor. Instale parches de seguridad críticos en el plazo de un mes a partir del lanzamiento. Nota: Los parches de seguridad críticos deben identific arse de acuerdo con el proceso de clasificación de riesgos definido en el requisito 6.1.	redshift-cluster-m aintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configura ción preferida para su organización. En concreto, que tengan períodos de mantenimi ento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrad e El valor predeterm inado es true. También te permite configurar de forma opcional el periodo preferredMaintenan ceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3.2	Revise el código personalizado antes de implementarlo en producción o de presentárselo a los clientes para identific ar cualquier posible vulnerabilidad de codificación (mediante procesos manuales o automatizados) e incluya al menos lo siguiente: • Los cambios de código los revisan personas distintas del autor del código original y personas que conocen las técnicas de revisión del código y las prácticas de codificación segura. • Las revisiones del código garantiza n que el código se desarrolle de acuerdo con las pautas de codificación segura • Se implementan las correcciones adecuadas antes de su publicación. • El personal responsab	ecr-private-image-scanning-habilitado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identific ar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	le revisa y aprueba los resultados de la revisión del código antes de su publicaci ón. (Continúa en la página siguiente)		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.6	En el caso de las aplicaciones web orientadas al público, aborde las nuevas amenazas y vulnerabilidades de forma continua y asegúrese de que estas aplicaciones estén protegidas contra los ataques conocidos mediante uno de los siguientes métodos: • Revisión de las aplicaciones web orientadas al público mediante herramientas o métodos manuales o automatizados de evaluación de la seguridad de las vulnerabilidades de las aplicaciones, al menos una vez al año y después de cualquier cambio. Nota: Esta evaluación no es lo mismo que los análisis de vulnerabilidades realizados para el requisito 11.2. • Instalación de una	alb-desync-mode-check	Para ayudar a proteger las aplicaciones contra las vulnerabilidades de desincronización HTTP, asegurar que el modo de mitigación de desincronización HTTP esté habilitado en los equilibradores de carga de aplicación. Los problemas de desincronización de HTTP pueden provocar el contrabando de solicitudes y hacer que sus aplicaciones sean vulnerables al envenenamiento de las colas de solicitudes o de la caché. La mitigación de desincronización incluye modos monitoreados, defensivos y más estrictos. El modo defensivo es el modo predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	solución técnica automatizada que detecte y prevenga los ataques basados en la web (por ejemplo, un firewall de aplicaciones web) frente a las aplicacio nes web públicas, para comprobar continuamente todo el tráfico.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.6	En el caso de las aplicaciones web orientadas al público, aborde las nuevas amenazas y vulnerabilidades de forma continua y asegúrese de que estas aplicaciones estén protegidas contra los ataques conocidos mediante uno de los siguientes métodos: • Revisión de las aplicaciones web orientadas al público mediante herramientas o métodos manuales o automatizados de evaluación de la seguridad de las vulnerabilidades de las aplicaciones, al menos una vez al año y después de cualquier cambio. Nota: Esta evaluación no es lo mismo que los análisis de vulnerabilidades realizados para el requisito 11.2. • Instalación de una	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en los Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	solución técnica automatizada que detecte y prevenga los ataques basados en la web (por ejemplo, un firewall de aplicaciones web) frente a las aplicacio nes web públicas, para comprobar continuamente todo el tráfico.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.6	En el caso de las aplicaciones web orientadas al público, aborde las nuevas amenazas y vulnerabilidades de forma continua y asegúrese de que estas aplicaciones estén protegidas contra los ataques conocidos mediante uno de los siguientes métodos: • Revisión de las aplicaciones web orientadas al público mediante herramientas o métodos manuales o automatizados de evaluación de la seguridad de las vulnerabilidades de las aplicaciones, al menos una vez al año y después de cualquier cambio. Nota: Esta evaluación no es lo mismo que los análisis de vulnerabilidades realizados para el requisito 11.2. • Instalación de una	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	solución técnica automatizada que detecte y prevenga los ataques basados en la web (por ejemplo, un firewall de aplicaciones web) frente a las aplicacio nes web públicas, para comprobar continuamente todo el tráfico.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.6	En el caso de las aplicaciones web orientadas al público, aborde las nuevas amenazas y vulnerabilidades de forma continua y asegúrese de que estas aplicaciones estén protegidas contra los ataques conocidos mediante uno de los siguientes métodos: • Revisión de las aplicaciones web orientadas al público mediante herramientas o métodos manuales o automatizados de evaluación de la seguridad de las vulnerabilidades de las aplicaciones, al menos una vez al año y después de cualquier cambio. Nota: Esta evaluación no es lo mismo que los análisis de vulnerabilidades realizados para el requisito 11.2. • Instalación de una	waf-regional-rule-not-vacío	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencadenar un comportamiento no deseado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	solución técnica automatizada que detecte y prevenga los ataques basados en la web (por ejemplo, un firewall de aplicaciones web) frente a las aplicacio nes web públicas, para comprobar continuamente todo el tráfico.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.6	En el caso de las aplicaciones web orientadas al público, aborde las nuevas amenazas y vulnerabilidades de forma continua y asegúrese de que estas aplicaciones estén protegidas contra los ataques conocidos mediante uno de los siguientes métodos: • Revisión de las aplicaciones web orientadas al público mediante herramientas o métodos manuales o automatizados de evaluación de la seguridad de las vulnerabilidades de las aplicaciones, al menos una vez al año y después de cualquier cambio. Nota: Esta evaluación no es lo mismo que los análisis de vulnerabilidades realizados para el requisito 11.2. • Instalación de una	waf-regional-rulegroup-not-vacío	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportamiento no deseado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	solución técnica automatizada que detecte y prevenga los ataques basados en la web (por ejemplo, un firewall de aplicaciones web) frente a las aplicacio nes web públicas, para comprobar continuamente todo el tráfico.		

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.6	En el caso de las aplicaciones web orientadas al público, aborde las nuevas amenazas y vulnerabilidades de forma continua y asegúrese de que estas aplicaciones estén protegidas contra los ataques conocidos mediante uno de los siguientes métodos: • Revisión de las aplicaciones web orientadas al público mediante herramientas o métodos manuales o automatizados de evaluación de la seguridad de las vulnerabilidades de las aplicaciones, al menos una vez al año y después de cualquier cambio. Nota: Esta evaluación no es lo mismo que los análisis de vulnerabilidades realizados para el requisito 11.2. • Instalación de una	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	solución técnica automatizada que detecte y prevenga los ataques basados en la web (por ejemplo, un firewall de aplicaciones web) frente a las aplicacio nes web públicas, para comprobar continuamente todo el tráfico.		
7.1.1	Defina las necesidad es de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegi o requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegi o mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomienda utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	ecs-containers-nonprivileged	Para ayudar a implementar el principio de privilegio mínimo, las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitados los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	ecs-containers-readonly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegio mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	efs-access-point-enforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	efs-access-point-enforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidad es de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegi o requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.1	Defina las necesidades de acceso para cada función, incluidos: • Los componentes del sistema y los recursos de datos a los que cada función debe acceder para su función laboral. • El nivel de privilegio requerido (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporciona mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearch Permite un control de acceso al dominio basado en funciones, así como una seguridad a nivel de índices, documentos y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.2	Restrinja el acceso al usuario privilegiado IDs al mínimo de los privilegios necesarios para desempeñar sus responsabilidades laborales.	iam-customer-policy-blocked-kms-acciones	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, lo que impide que las políticas contengan acciones bloqueadas en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el blockedActionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
7.1.2	Restrinja el acceso al usuario privilegiado IDs al mínimo de los privilegios necesarios para desempeñar sus responsabilidades laborales.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.2	Restrinja el acceso al usuario privilegiado IDs al mínimo de los privilegios necesario s para desempeñar sus responsabilidades laborales.	iam-inline-policy-blocked-kms-acciones	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
7.1.2	Restrinja el acceso al usuario privilegiado IDs al mínimo de los privilegios necesario s para desempeñar sus responsabilidades laborales.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.2	Restrinja el acceso al usuario privilegiado IDs al mínimo de los privilegios necesarios para desempeñar sus responsabilidades laborales.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.2	Restrinja el acceso al usuario privilegiado IDs al mínimo de los privilegios necesarios para desempeñar sus responsabilidades laborales.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
7.1.2	Restrinja el acceso al usuario privilegiado IDs al mínimo de los privilegios necesarios para desempeñar sus responsabilidades laborales.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.2	Restrinja el acceso al usuario privilegiado IDs al mínimo de los privilegios necesarios para desempeñar sus responsabilidades laborales.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.1.2	Restrinja el acceso al usuario privilegiado IDs al mínimo de los privilegios necesario s para desempeñar sus responsabilidades laborales.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	ecs-containers-non privileged	Para ayudar a implementar el principio de privilegio mínimo, las definicio nes de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitad os los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegi os elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	ecs-containers-rea donly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegi o mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	efs-access-point-e nforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringi r el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	efs-access-point-e nforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configura da en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los componentes del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específicamente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los componentes del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específicamente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	iam-user-group-mem bership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizac iones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separació n de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en «denegar todo» a menos que se permita específic amente. Este sistema o sistemas de control de acceso deben incluir lo siguiente: cobertura de todos los componentes del sistema.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	ecs-containers-non privileged	Para ayudar a implementar el principio de privilegio mínimo, las definicio nes de tareas de Amazon Elastic Container Service (Amazon ECS) no deben tener habilitad os los privilegios elevados. Cuando este parámetro es verdadero, al contenedor se le conceden privilegi os elevados en la instancia de contenedor de host, similares a los de un usuario raíz.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	ecs-containers-rea donly-access	Habilitar el acceso de solo lectura a los contenedores de Amazon Elastic Container Service (ECS) puede ayudar a cumplir con el principio de privilegi o mínimo. Esta opción puede reducir los vectores de ataque, ya que el sistema de archivos de la instancia de contenedor no se puede modificar a menos que tenga permisos explícitos de lectura y escritura.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	efs-access-point-e nforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringi r el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	efs-access-point-e nforce-identidad de usuario	Para ayudar a implementar el principio del privilegio mínimo, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configura da en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, lo que impide que las políticas contengan acciones bloqueada s en todas AWS las claves del Servicio de administración de claves. Tener más privilegios de los necesario s para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política en línea que permita bloquear acciones en todas las claves del Servicio de administración de claves. AWS AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos. Esta regla le permite establece r el blockedAc tionsPatterns parámetro. (Valor AWS fundamental de las mejores prácticas de seguridad: kms: descifrar, kms:ReEnc

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			ryptFrom). Los valores reales deben reflejar las políticas de su organización.
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Managemen t) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los componentes del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignación de privilegios a personas en función de la clasificación y la función de los puestos.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los componentes del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignación de privilegios a personas en función de la clasificación y la función de los puestos.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	iam-root-access-key-compruebe	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los componentes del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignación de privilegios a personas en función de la clasificación y la función de los puestos.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	Establezca un sistema o sistemas de control de acceso para los component es del sistema que restrinja el acceso en función de la necesidad de datos del usuario y esté configurado en “denegar todo” a menos que se permita específicamente. Estos sistemas de control de acceso deben incluir lo siguiente: Asignació n de privilegios a personas en función de la clasificación y la función de los puestos.	opensearch-access-control-enabled	Asegúrese de que el control de acceso detallado esté habilitado en sus dominios de Amazon OpenSearch Service. El control de acceso detallado proporcio na mecanismos de autorización mejorados para lograr el acceso con menos privilegios a los dominios de Amazon Service. OpenSearc h Permite un control de acceso al dominio basado en funciones , así como una seguridad a nivel de índices, documento s y campos, la compatibilidad con los paneles de servicio, la multitenencia y la autenticación básica HTTP para OpenSearch Service y Kibana. OpenSearc h

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.3	Configuración predeterminada de “denegar todo”.	s3- bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1.1	Asigne a todos los usuarios un identific ador único antes de permitirles acceder a los componentes del sistema o a los datos del titular de la tarjeta.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1.4	Elimine o desactive las cuentas de usuario inactivas en un plazo de 90 días.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	codebuild-project-environment-privileged-comprobar	Para ayudarte a implementar el principio de privilegios mínimos, asegúrate de que el entorno de tu CodeBuild proyecto de Amazon no tenga activado el modo privilegiado. Esta configuración debe estar deshabili tada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	ecs-no-environment-secrets	Como práctica recomendada de seguridad, transmita información confidenc ial a contenedores como variables de entorno. Puede inyectar datos de forma segura en sus contenedores de Amazon Elastic Container Service (ECS) haciendo referencia a los valores almacenad os en AWS Systems Manager Parameter Store o AWS Secrets Manager en la definición de contenedor de una definición de tarea de Amazon ECS. A continuación, puede exponer la informaci ón confidencial como variables de entorno o en la configuración de registro de un contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	efs-encrypted-check	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	elasticsearch-encr ypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configura dos con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	encrypted-volumes	Puesto que puede haber datos confidenc iales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	opensearch-encrypt ed-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	rds-snapshot-encry pted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitado para sus instancias de Amazon Relationa l Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	redshift-cluster-c onfiguration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configura ciones necesaria s se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	Habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	s3- bucket-ssl-request s-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitud es para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	sagemaker-endpoint -configuration-kms- configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	sagemaker-notebook -instance-kms-conf igurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administr ación de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	secretsmanager-usi ng-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para AWS los secretos de Secrets Manager. Puesto que puede haber datos confidenc iales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	Mediante criptografía fuerte, haga ilegibles todas las credencia les de autenticación (como contraseñ as/frases) durante la transmisión y el almacenamiento en todos los component es del sistema.	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administración de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.3	Las contraseñas/frases de contraseña deben cumplir los siguientes requisitos: • Deben tener una longitud mínima de siete caracteres. • Contener caracteres numéricos y alfabéticos. Como alternativa, las contraseñas/frases de contraseña deben tener una complejidad y una seguridad al menos equivalentes a las de los parámetros especificados anteriormente.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (PCI DSS predeterminado: falso), RequireLowercaseCharacters (PCI DSS predeterminado: verdadero), RequireSymbols (PCI DSS predeterminado: falso), RequireNumbers (PCI DSS predeterm

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			inado: verdadero), MinimumPa sswordLength (PCI DSS predeterm inado: 7), PasswordR eusePrevention (PCI DSS predeterminado: 4) y MaxPasswo rdAge (PCI DSS predeterminado: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.4	Cambie passwords /passphrases de usuario al menos cada 90 días.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.4	Cambie de usuario passwords/passphrases al menos cada 90 días.	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configurar opcionalmente RequireUppercaseCharacters (PCI DSS predeterminado: falso), RequireLowercaseCharacters (PCI DSS predeterminado: verdadero), RequireSymbols (PCI DSS predeterminado: falso), RequireNumbers (PCI DSS predeterm

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			inado: verdadero), MinimumPa sswordLength (PCI DSS predeterm inado: 7), PasswordR eusePrevention (PCI DSS predeterminado: 4) y MaxPasswo rdAge (PCI DSS predeterminado: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.
8.2.4	Cambie passwords /passphrases de usuario al menos cada 90 días.	secretsmanager-rot ation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencial mente, reducir el impacto sobre la empresa si el secreto se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.5	No permitas que una persona envíe una nueva password/ passphrase que sea igual a cualquiera de las cuatro passwords /passphrases últimas que ha utilizado.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (PCI DSS predeterminado: falso), RequireLo wercaseCharacters (PCI DSS predeterm inado: verdadero), RequireSymbols (PCI DSS predeterm inado: falso), RequireNumbers (PCI DSS predeterm

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			inado: verdadero), MinimumPa sswordLength (PCI DSS predeterm inado: 7), PasswordR eusePrevention (PCI DSS predeterminado: 4) y MaxPasswo rdAge (PCI DSS predeterminado: 90) para su política de contraseñas de IAM. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.1	Incorpore la autenticación multifactor para todos los accesos que no sean de consola en el CDE para el personal con acceso administrativo.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.1	Incorpore la autenticación multifactor para todos los accesos que no sean de consola en el CDE para el personal con acceso administrativo.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.1	Incorpore la autenticación multifactor para todos los accesos que no sean de consola en el CDE para el personal con acceso administrativo.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.1	Incorpore la autenticación multifactor para todos los accesos que no sean de consola en el CDE para el personal con acceso administrativo.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Incorpore la autenticación multifactor para todos los accesos remotos a la red (tanto de usuario como de administrador, e incluido el acceso de terceros para soporte o mantenimiento) que se originen fuera de la red de la entidad.	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Incorpore la autenticación multifactor para todos los accesos remotos a la red (tanto de usuario como de administrador, e incluido el acceso de terceros para soporte o mantenimiento) que se originen fuera de la red de la entidad.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Incorpore la autenticación multifactor para todos los accesos remotos a la red (tanto de usuario como de administrador, e incluido el acceso de terceros para soporte o mantenimiento) que se originen fuera de la red de la entidad.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Incorpore la autenticación multifactor para todos los accesos remotos a la red (tanto de usuario como de administrador, e incluido el acceso de terceros para soporte o mantenimiento) que se originen fuera de la red de la entidad.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilaci ón se envíen a Amazon CloudWatc h o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.1	Implemente registros de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todos los usuarios individuales acceden a los datos del titular de la tarjeta	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todas las acciones realizadas por cualquier persona con privilegios de administrador o raíz	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todas las acciones realizadas por cualquier persona con privilegios de administrador o raíz	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todas las acciones realizadas por cualquier persona con privilegios de administrador o raíz	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todas las acciones realizadas por cualquier persona con privilegios de administrador o raíz	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todas las acciones realizadas por cualquier persona con privilegios de administrador o raíz	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todas las acciones realizadas por cualquier persona con privilegios de administrador o raíz	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todas las acciones realizadas por cualquier persona con privilegios de administrador o raíz	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: todas las acciones realizadas por cualquier persona con privilegios de administrador o raíz	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.3	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: acceso a todos los registros de seguimiento de auditoría	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.4	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: intentos de acceso lógico no válidos	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.5	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: uso y cambios en los mecanismos de identificación y autenticación, incluyendo pero no limitado a la creación de nuevas cuentas y elevación de privilegios, y todos los cambios, adiciones o eliminaciones en cuentas con privilegios de administrador o raíz	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.5	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: uso y cambios en los mecanismos de identificación y autenticación, incluyendo pero no limitado a la creación de nuevas cuentas y elevación de privilegios, y todos los cambios, adiciones o eliminaciones en cuentas con privilegios de administrador o raíz	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.5	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: uso y cambios en los mecanismos de identificación y autenticación, incluyendo pero no limitado a la creación de nuevas cuentas y elevación de privilegios, y todos los cambios, adiciones o eliminaciones en cuentas con privilegios de administrador o raíz	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.5	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: uso y cambios en los mecanismos de identificación y autenticación, incluyendo pero no limitado a la creación de nuevas cuentas y elevación de privilegios, y todos los cambios, adiciones o eliminaciones en cuentas con privilegios de administrador o raíz	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.5	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: uso y cambios en los mecanismos de identificación y autenticación, incluyendo pero no limitado a la creación de nuevas cuentas y elevación de privilegios, y todos los cambios, adiciones o eliminaciones en cuentas con privilegios de administrador o raíz	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.5	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: uso y cambios en los mecanismos de identificación y autenticación, incluyendo pero no limitado a la creación de nuevas cuentas y elevación de privilegios, y todos los cambios, adiciones o eliminaciones en cuentas con privilegios de administrador o raíz	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.5	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: uso y cambios en los mecanismos de identificación y autenticación, incluyendo pero no limitado a la creación de nuevas cuentas y elevación de privilegios, y todos los cambios, adiciones o eliminaciones en cuentas con privilegios de administrador o raíz	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
102.5	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: uso y cambios en los mecanismos de identificación y autenticación, incluyendo pero no limitado a la creación de nuevas cuentas y elevación de privilegios, y todos los cambios, adiciones o eliminaciones en cuentas con privilegios de administrador o raíz	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.6	Implemente los registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: inicialización, detención o pausa de los registros de auditoría	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.6	Implemente los registros de auditoría automatizados para que todos los componentes del sistema reconstru yan los siguientes eventos: inicialización, detención o pausa de los registros de auditoría	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.6	Implemente los registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: inicialización, detención o pausa de los registros de auditoría	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
10.2.7	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: creación y eliminación de objetos en el nivel del sistema	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.7	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: creación y eliminación de objetos en el nivel del sistema	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.7	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: creación y eliminación de objetos en el nivel del sistema	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.7	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: creación y eliminación de objetos en el nivel del sistema	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.7	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: creación y eliminación de objetos en el nivel del sistema	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.7	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: creación y eliminación de objetos en el nivel del sistema	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.7	Implemente registros de auditoría automatizados para que todos los componentes del sistema reconstruyan los siguientes eventos: creación y eliminación de objetos en el nivel del sistema	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web regional y global. ACLs AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola de AWS administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilaci ón se envíen a Amazon CloudWatc h o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Registre al menos las siguientes entradas de registros de auditoría para todos los componentes del sistema para cada evento: identificación del usuario	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5	Proteja los registros de auditoría para que no se puedan modificar.	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros. AWS CloudTrail
10.5	Proteja los registros de auditoría para que no se puedan modificar.	habilitado para bucket-server-side-encryption s3	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5	Proteja los registros de auditoría para que no se puedan modificar.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
10.5.2	Proteja los archivos de registros de auditoría frente a modificaciones no autorizadas.	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.2	Proteja los archivos de registros de auditoría frente a modificaciones no autorizadas.	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
10.5.2	Proteja los archivos de registros de auditoría frente a modificaciones no autorizadas.	s3- default-encryption -kms	Asegúrese de tener el cifrado habilitad o para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.3	Haga rápidamente copias de seguridad de los archivos de registro de seguimiento de auditoría en un servidor de registro centralizado o en un medio que sea difícil de modificar.	s3- lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.3	Haga rápidamente copias de seguridad de los archivos de registro de seguimiento de auditoría en un servidor de registro centralizado o en un medio que sea difícil de modificar.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
10.5.3	Haga rápidamente copias de seguridad de los archivos de registro de seguimien to de auditoría en un servidor de registro centralizado o en un medio que sea difícil de modificar.	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.3	Haga rápidamente copias de seguridad de los archivos de registro de seguimien to de auditoría en un servidor de registro centralizado o en un medio que sea difícil de modificar.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincróni ca para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.5	Utilice software de monitoreo de integrida d de archivos o de detección de cambios en los registros para asegurarse de que los datos de registro existentes no se puedan cambiar sin generar alertas (aunque la agregació n de nuevos datos no debería generar alertas).	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrai l La validación del archivo de registro ayuda a determina r si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsifica r los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.5	Utilice software de monitoreo de integrida d de archivos o de detección de cambios en los registros para asegurarse de que los datos de registro existentes no se puedan cambiar sin generar alertas (aunque la agregació n de nuevos datos no debería generar alertas).	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenad os en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilment e de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7	Retenga el registro de auditoría durante al menos un año, con un mínimo de tres meses disponible de forma inmediata para su análisis (por ejemplo, en línea, archivado o recuperable a partir de una copia de seguridad).	s3- lifecycle-policy-check	Asegúrese de que las políticas de ciclo de vida de Amazon S3 estén configuradas para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo: la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7	Retenga el registro de auditoría durante al menos un año, con un mínimo de tres meses disponible de forma inmediata para su análisis (por ejemplo, en línea, archivado o recuperable a partir de una copia de seguridad).	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
11.2.3	Realice escaneos internos y externos, y vuelva a escanear según sea necesario después de cualquier cambio significativo. Los escaneos deben ser realizados por personal cualificado.	ecr-private-image-scanning-habilitado	El análisis de imágenes de Amazon Elastic Container Repository (ECR) ayuda a identific ar vulnerabilidades de software en las imágenes de contenedor. Al habilitar el análisis de imágenes en los repositorios de ECR, se añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Utilice técnicas de detección y and/or prevención de intrusiones para detectar e and/or impedir las intrusiones en la red. Supervise todo el tráfico en el perímetro del entorno de datos del titular de la tarjeta, así como en los puntos críticos del entorno de datos del titular de la tarjeta, y avise al personal en caso de que se sospeche que se ha producido algún riesgo. Mantenga actualizados todos los motores de detección y prevención de intrusiones, las bases de referencia y las firmas.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.4	Utilice técnicas de detección y and/or prevención de intrusiones para detectar e and/or impedir las intrusiones en la red. Supervise todo el tráfico en el perímetro del entorno de datos del titular de la tarjeta, así como en los puntos críticos del entorno de datos del titular de la tarjeta, y avise al personal en caso de que se sospeche que se ha producido algún riesgo. Mantenga actualizados todos los motores de detección y prevención de intrusiones, las bases de referencia y las firmas.	netfw-policy-rule-group-asociado	Una política AWS de Network Firewall define la forma en que su firewall supervisa y gestiona el tráfico en una Amazon VPC. Puede configurar grupos de reglas sin y con estado para filtrar los paquetes y los flujos de tráfico, y definir la administr ación del tráfico predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.5	Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de supervisión de la integridad de los archivos) para alertar al personal sobre cualquier modificación no autorizada (incluidos cambios, adiciones y eliminaciones) de archivos críticos del sistema, archivos de configuración o archivos de contenido; y configure el software para que realice comparaciones de archivos importantes al menos una vez por semana.	cloud-trail-log-file-habilitado para la validación	Utilice la validación de los archivos de AWS CloudTrail registro para comprobar la integridad de los registros. CloudTrail La validación del archivo de registro ayuda a determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregarlo. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, eliminar o falsificar los archivos de CloudTrail registro sin ser detectados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.5	Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de supervisión de la integridad de los archivos) para alertar al personal sobre cualquier modificación no autorizada (incluidos cambios, adiciones y eliminaciones) de archivos críticos del sistema, archivos de configuración o archivos de contenido; y configure el software para que realice comparaciones de archivos importantes al menos una vez por semana.	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para PCI DSS 3.2.1.

Prácticas operativas recomendadas para el PCI DSS 4.0 (excluye los tipos de recursos globales)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costos mediante reglas

administradas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) 4.0 (excluidos los tipos de recursos globales) y las reglas de AWS Config administradas. Cada AWS Config regla se aplica a un AWS recurso específico y se refiere a uno o más controles de PCI DSS. Un control del PCI DSS puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.5	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	Asegúrese de que un servidor creado con AWS Transfer Family no utilice FTP para la conexión de punto final. La regla es NON_COMPLIANT si el protocolo del servidor para la conexión del punto de conexión está habilitado para FTP.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpointConfigurationType'. La regla devuelve NON_COMPLIANT

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING_SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferentes. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario, es NON_COMPLIANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociados a las listas de control de acceso AWS WAFv2 web (ACLs). La regla no es compatibl e con una AWS AppSync API si no está asociada a una ACL web.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPL IANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no cumple con los requisitos si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRoutin g' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING_SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferentes. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario, es NON_COMPLIANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociados a las listas de control de acceso a la AWS WAFv2 web ()ACLs. La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRoutin g' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING_SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferentes. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario, es NON_COMPLIANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociados a las listas de control de acceso a la AWS WAFv2 web ()ACLs. La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.1	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
1.4.1	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRouting' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.1	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFron t distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRouting' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING _SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferente s. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario , es NON_COMPL IANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociados a las listas de control de acceso a la AWS WAFv2 web ()ACLs. La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.3	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.3	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.3	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes completos	Asegúrese de que la política de AWS Network Firewall esté configurada con una acción sin estado predeterminada definida por el usuario para los paquetes completos. La regla es NON_COMPLIANT si la acción predeterminada sin estado para los paquetes completos no coincide con la acción predeterminada sin estado definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.4	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
1.4.4	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRouting' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.4	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.
1.4.5	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	ecs-task-definition-pid-comprobación de modo	Asegúrese de que ECSTask las definiciones estén configuradas para compartir el espacio de nombres de procesos de un host con sus contenedores de Amazon Elastic Container Service (Amazon ECS). La regla es NON_COMPLIANT si el parámetro pidMode está establecido en “host”.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.5	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	ec2- -deshabilitado launch-template-public-ip	Compruebe que las plantillas de lanzamiento de Amazon EC2 no estén configuradas para asignar direcciones IP públicas a interfaces de red. La regla no cumple con los requisitos si la versión predeterminada de una plantilla de lanzamiento de EC2 tiene al menos una interfaz de red con el valor «verdadero». AssociatePublicIpAddress

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpointConfigurationType'. La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmentados. La regla es NON_COMPLIANT si la acción predeterminada sin estado para los paquetes fragmentados no coincide con la acción predeterminada definida por el usuario.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING_SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferentes. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario, es NON_COMPLIANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso AWS WAFv2 web ()ACLs. La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.2.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitado la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
102.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definicio nes de tareas de Amazon ECS. Esta regla no es compatibl e si una ECSTask definición activa no tiene definido el recurso LogConfig uration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
102.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsE nabledel campo 'está establecido en falso.
10.2.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
102.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.2.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
102.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.2.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
102.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.2.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.2.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TRAIL_ENABLED) y el nombre de la regla (cloudtrail-enabled) son diferentes. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimiento habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimien to que cumpla todos los requisitos siguientes:
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibido	Compruebe que haya una instantán ea manual de un clúster de base de datos de Amazon Neptune que no sea pública. La regla es NON_COMPLIANT si las instantáneas de clústeres nuevas y existentes de Neptune son públicas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla es NON_COMPLIANT si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	aurora-resources-protected-by-plan de respaldo	Compruebe que los clústeres de bases de datos de Amazon Aurora estén protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el clúster de bases de datos de Amazon Relational Database Service (Amazon RDS) no está protegido por un plan de copia de seguridad.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	db-instance-backup-enabled	Compruebe que las instancias de base de datos de RDS tengan habilitada la copia de seguridad. Opcionalmente, la regla comprueba el periodo de retención de copia de seguridad y el periodo de tiempo de la copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	dynamodb-in-backup-plan	Asegúrese de que las tablas de Amazon DynamoDB estén presentes en AWS los planes de Backup. La regla no es conforme si las tablas de Amazon DynamoDB no están presentes en ningún plan de Backup. AWS
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	dynamodb-resources-protected-by-plan de respaldo	Compruebe que las tablas de Amazon DynamoDB estén protegidas por un plan de copia de seguridad. La regla es NON_COMPLIANT si la tabla de DynamoDB no está cubierta por un plan de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	ebs-in-backup-plan	Asegúrese de añadir los volúmenes de Amazon Elastic Block Store (Amazon EBS) a los planes de backup de Backup. AWS La regla es NON_COMPLIANT si los volúmenes de Amazon EBS no están incluidos en los planes de copia de seguridad.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	ebs-resources-protected-by-plan de respaldo	Compruebe que los volúmenes de Amazon Elastic Block Store (Amazon EBS) estén protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el volumen de Amazon EBS no está cubierto por un plan de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	ec2- -plan resources-protected-by-backup	Compruebe que las instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén protegidas por un plan de copia de seguridad. La regla es NON_COMPLIANT si la instancia de Amazon EC2 no está cubierta por un plan de copia de seguridad.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	efs-resources-protected-by-plan de respaldo	Compruebe que los sistemas de archivos de Amazon Elastic File System (Amazon EFS) estén protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el sistema de archivos de EFS no está cubierto por un plan de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	elasticache-redis-cluster-automatic-verificación de respaldo	Compruebe si los clústeres de Amazon ElastiCache Redis tienen activada la copia de seguridad automática. La regla no es compatible si el clúster SnapshotRetentionLimit de Redis es inferior al parámetro. SnapshotRetentionPeriod Por ejemplo: si el parámetro es 15, la regla no es compatible si está entre 0 y 15. snapshotRetentionPeriod
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	fsx-resources-protected-by-plan de respaldo	Asegúrese de que Amazon FSx File Systems esté protegido por un plan de respaldo. La regla no cumple con los requisitos si el sistema de FSx archivos de Amazon no está cubierto por un plan de respaldo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	neptune-cluster-backup-retention-comprobar	Compruebe que el período de retención de un clúster de base de datos de Amazon Neptune se haya configurado a un número específico de días. La regla es NON_COMPLIANT si el período de retención es inferior al valor especificado por el parámetro.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	rds-in-backup-plan	Asegúrese de que las bases de datos de Amazon Relational Database Service (Amazon RDS) estén presentes en los planes de AWS Backup. La regla no es conforme si las bases de datos de Amazon RDS no están incluidas en ningún plan de Backup AWS .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	redshift-backup-enabled	Compruebe que las instantáneas automatizadas de Amazon Redshift estén habilitadas para clústeres. La regla no es compatible si el valor del automated SnapshotRetention período es mayor MaxRetentionPeriod o menor que MinRetentionPeriod o el valor es 0.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	plan s3 resources-protected-by-backup	Compruebe que los buckets de Amazon Simple Storage Service (Amazon S3) estén protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el bucket de Amazon S3 no está cubierto por un plan de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimien to que cumpla todos los requisitos siguientes:
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	db-instance-backup-enabled	Compruebe que las instancias de base de datos de RDS tengan habilitada la copia de seguridad . Opcionalmente, la regla comprueba el periodo de retención de copia de seguridad y el periodo de tiempo de la copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.
10.3.4	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	s3- bucket-default-lock-enabled	Compruebe que el bucket de S3 tenga habilitado el bloqueo de forma predeterminada. La regla es NON_COMPLIANT si el bloqueo no está habilitado.
10.3.4	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	s3- bucket-versioning-enabled	Compruebe que se haya habilitado el control de versiones para los buckets de S3. Opcionalmente, la regla comprueba si la eliminación de MFA está habilitada para los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.4	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimien to que cumpla todos los requisitos siguientes:
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-r esource-check	Asegúrese de que un tipo de recurso tenga una CloudWatc h alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsE nabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-r esource-check	Asegúrese de que un tipo de recurso tenga una CloudWatc h alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsE nabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-r esource-check	Asegúrese de que un tipo de recurso tenga una CloudWatc h alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsE nabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.3	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimiento que cumpla todos los requisitos siguientes:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definicio nes de tareas de Amazon ECS. Esta regla no es compatibl e si una ECSTask definición activa no tiene definido el recurso LogConfig uration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TRAIL_ENABLED) y el nombre de la regla (cloudtrail-enabled) son diferentes. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimiento habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.5.2	Las intrusiones en la red y los cambios inesperados en los archivos se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.5.2	Las intrusiones en la red y los cambios inesperados en los archivos se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.
11.5.2	Las intrusiones en la red y los cambios inesperados en los archivos se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan la configuración especificada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.5.2	Las intrusiones en la red y los cambios inesperados en los archivos se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.6.1	Los cambios no autorizados en las páginas de pago se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.6.1	Los cambios no autorizados en las páginas de pago se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.
11.6.1	Los cambios no autorizados en las páginas de pago se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan la configuración especificada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.6.1	Los cambios no autorizados en las páginas de pago se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.10.5	Se responde inmediatamente a los incidentes de seguridad, sospechosos y confirmados, que puedan afectar al CDE. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.10.5	Se responde inmediatamente a los incidentes de seguridad, sospechosos y confirmados, que puedan afectar al CDE. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.
12.10.5	Se responde inmediatamente a los incidentes de seguridad, sospechosos y confirmados, que puedan afectar al CDE. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan la configuración especificada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.10.5	Se responde inmediatamente a los incidentes de seguridad, sospechosos y confirmados, que puedan afectar al CDE. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.
12.4.2.1	El cumplimiento de PCI DSS está administrado. (PCI-DSS-v4.0)	service-catalog-shared-within-organización	Asegúrese de que AWS Service Catalog comparta las carteras con una organización (un conjunto de AWS cuentas tratadas como una sola unidad) cuando la integración esté habilitada con AWS Organizations. La regla es NON_COMPLIANT si el valor de Tipo al compartir es ACCOUNT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.5	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	Asegúrese de que un servidor creado con AWS Transfer Family no utilice FTP para la conexión de punto final. La regla es NON_COMPL IANT si el protocolo del servidor para la conexión del punto de conexión está habilitado para FTP.
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) de los almacenes de datos de Redis estén habilitados para el TLS/SSL cifrado de los datos comunicad os con otros puntos finales. La regla no cumple con los requisitos si el cifrado no está activado. TLS/SSL

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	msk-in-cluster-node-requerido-tls	Compruebe que haya un clúster de Amazon MSK que aplique el cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) estén configurados con una conexión SSL. La regla NO ES COMPATIBLE si el AWS DMS no tiene configurada una conexión SSL.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1	El almacenamiento de los datos de la cuenta se reduce al mínimo. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.
3.2.1	El almacenamiento de los datos de la cuenta se reduce al mínimo. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1	El almacenamiento de los datos de la cuenta se reduce al mínimo. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.
3.2.1	El almacenamiento de los datos de la cuenta se reduce al mínimo. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1.1	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.
3.3.1.1	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1.1	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.
3.3.1.1	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.
3.3.1.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.
3.3.1.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.
3.3.2	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.
3.3.2	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.
3.3.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.
3.3.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-descanso	Compruebe que haya un grupo de trabajo de Amazon Athena cifrado en reposo. La regla es NON_COMPLIANT si el cifrado de datos en reposo no está habilitado para un grupo de trabajo de Athena.
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Compruebe que haya un clúster de base de datos de Amazon Neptune con instantáneas cifradas. La regla es NON_COMPLIANT si un clúster de Neptune no tiene las instantáneas cifradas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Asegúrese de que los clústeres de Amazon Redshift utilicen una AWS clave específica del Servicio de administración de claves (AWS KMS) para el cifrado. La regla cumple con las normas si el cifrado está activado y el clúster está cifrado con la clave proporcionada en el kmsKeyArn parámetro. La regla es NON_COMPLIANT si el clúster no está cifrado o está cifrado con otra clave.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	codebuild-project-sCifrado de 3 registros	Asegúrese de que un AWS CodeBuild proyecto configura do con Amazon S3 Logs tenga el cifrado activado para sus registros. La regla no es compatible si 'EncryptionDisabled' se establece en 'true' en el S3 LogsConfi g de un proyecto. CodeBuild
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	eks-secrets-encrypted	Asegúrese de que los clústeres de Amazon Elastic Kubernetes Service estén configurados para cifrar AWS los secretos de Kubernetes mediante claves del Servicio de administración de claves (KMS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	api-gw-cache-enabled-y encriptado	Compruebe que todos los métodos de las etapas de Amazon API Gateway tengan memoria caché habilitada y cifrada. La regla es NON_COMPLIANT si algún método de una etapa de Amazon API Gateway no está configurada para el almacenamiento en caché o si la caché no está cifrada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Asegúrese de que la tabla de Amazon DynamoDB esté cifrada AWS con el Servicio de administración de claves (KMS). La regla no es compatible si la tabla de Amazon DynamoDB no está cifrada con KMS. AWS La regla tampoco cumple con los requisitos si la clave de AWS KMS cifrada no está presente en el parámetro de entrada. kmsKeyArns

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-comprobar	Asegúrese de que el proyecto NO contenga variables de entorno ni AWS_ACCESS_KEY_ID AWS_SECRET _ACCESS_KEY. La regla es NON_COMPLIANT si las variables de entorno del proyecto contienen credenciales de texto no cifrado.
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Asegúrese de que los clústeres de Amazon EKS no estén configurados para cifrar los secretos de Kubernetes mediante KMS. AWS La regla es NON_COMPLIANT si hay un clúster de EKS sin un recurso de encryptionConfig o si encryptionConfig no designa secretos como un recurso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Compruebe que los flujos de Amazon Kinesis estén cifrados en reposo con el cifrado en el servidor. La regla no cumple con las normas para una transmisión de Kinesis si 'StreamEncryption' no está presente.
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Compruebe que el cifrado de almacenamiento esté habilitado para los clústeres de base de datos de Amazon Neptune. La regla es NON_COMPLIANT si el cifrado de almacenamiento no está habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.5.1.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibido	Compruebe que haya una instantánea manual de un clúster de base de datos de Amazon Neptune que no sea pública. La regla es NON_COMPLIANT si las instantáneas de clústeres nuevas y existentes de Neptune son públicas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla es NON_COMPLIANT si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen puertos distintos del puerto 22. PermittedPublicSecurityGroupRuleRanges
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.6.1	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1.2	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.6.1.2	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1.3	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.6.1.3	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1.4	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.6.1.4	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.1	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-certificate-rsa-check	Asegúrese de que los certificados RSA administrados por AWS Certificate Manager (ACM) tengan una longitud de clave de al menos «2048» bits. La regla no es compatible si la longitud mínima de la clave es inferior a 2048 bits.
3.7.1	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS privada (CA AWS privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.1	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.2	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.2	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.4	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.4	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.6	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.6	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.7	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.7	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) de los almacenes de datos de Redis estén habilitados para el TLS/SSL cifrado de los datos comunicados con otros puntos finales. La regla no cumple con los requisitos si el cifrado no está activado. TLS/SSL

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	msk-in-cluster-node-requerido-tls	Compruebe que haya un clúster de Amazon MSK que aplique el cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) estén configurados con una conexión SSL. La regla NO ES COMPATIBLE si el AWS DMS no tiene configurada una conexión SSL.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) de los almacenes de datos de Redis estén habilitados para el TLS/SSL cifrado de los datos comunicados con otros puntos finales. La regla no cumple con los requisitos si el cifrado no está activado. TLS/SSL

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	msk-in-cluster-node-requerido-tls	Compruebe que haya un clúster de Amazon MSK que aplique el cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) estén configurados con una conexión SSL. La regla NO ES COMPATIBLE si el AWS DMS no tiene configurada una conexión SSL.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimiento que cumpla todos los requisitos siguientes:
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definicio nes de tareas de Amazon ECS. Esta regla no es compatibl e si una ECSTask definición activa no tiene definido el recurso LogConfig uration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3.3	Las vulnerabilidades de seguridad se identifican y se gestionan. (PCI-DSS-v4.0)	lambda-function-settings-check	Asegúrese de que la configuración de la función AWS Lambda para el tiempo de ejecución , la función, el tiempo de espera y el tamaño de la memoria coincidan con los valores esperados . La regla ignora las funciones con el tipo de paquete “Image” y las funciones con el tiempo de ejecución establecido en Tiempo de ejecución exclusivo del sistema operativo. La regla es NON_COMPLIANT si la configuración de la función de Lambda no coincide con los valores esperados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3.3	Las vulnerabilidades de seguridad se identifican y se gestionan. (PCI-DSS-v4.0)	eks-cluster-oldest-supported-versión	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (EKS) que no ejecute la versión compatible más antigua. La regla es NON_COMPL IANT si un clúster de EKS ejecuta la versión compatible más antigua (igual al parámetro oldestVer sionSupported).
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso a la AWS WAFv2 web (ACLs). La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	guerra 2- webacl-not-empty	Asegúrese de que una ACL WAFv2 web contenga cualquier regla de WAF o grupo de reglas de WAF. Esta regla NON_COMPLIANT si una ACL web no contiene reglas de WAF ni grupos de reglas de WAF.
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	guerra 2- rulegroup-not-empty	Asegúrese de que los WAFv2 grupos de reglas contengan reglas. La regla no es compatible si no hay reglas en un WAFv2 grupo de reglas.
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso a la AWS WAFv2 web (ACLs). La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	guerra 2- webacl-not-empty	Asegúrese de que una ACL WAFv2 web contenga cualquier regla de WAF o grupo de reglas de WAF. Esta regla NON_COMPLIANT si una ACL web no contiene reglas de WAF ni grupos de reglas de WAF.
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	guerra 2- rulegroup-not-empty	Asegúrese de que los WAFv2 grupos de reglas contengan reglas. La regla no es compatible si no hay reglas en un WAFv2 grupo de reglas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.5.5	Los cambios en todos los componentes del sistema se administr an de forma segura. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-turno desactivado	Compruebe que el grupo de implement ación de la plataform a de computación Lambda no utilice la configuración de implementación predeterminada. La regla no es compatibl e si el grupo de despliegue utiliza la configuración de despliegue '. CodeDeployDefault LambdaAllAtOnce'.
6.5.6	Los cambios en todos los componentes del sistema se administr an de forma segura. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-turno desactivado	Compruebe que el grupo de implement ación de la plataform a de computación Lambda no utilice la configuración de implementación predeterminada. La regla no es compatibl e si el grupo de despliegue utiliza la configuración de despliegue '. CodeDeployDefault LambdaAllAtOnce'.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.4	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específico o de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específico de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.6	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.6	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
8.2.1	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-comprobar	Asegúrese de que el proyecto NO contenga variables de entorno ni AWS_ACCES S_KEY_ID AWS_SECRE T _ACCESS_K EY. La regla es NON_COMPLIANT si las variables de entorno del proyecto contienen credencia les de texto no cifrado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se roten correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específico o de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.
8.2.4	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.4	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.
8.2.5	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.5	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.
8.2.6	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	secretsmanager-sec ret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específic o de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec2-imdsv2-check	Asegúrese de que la versión de metadatos de su instancia de Amazon Elastic Compute Cloud (Amazon EC2) esté configurada con la versión 2 () de Instance Metadata Service. IMDSv2 La regla no cumple con los requisitos si HttpTokens se establece en opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	autoscaling-launchconfig-requires-imdsv2.	Asegúrese de que solo IMDSv2 esté activado. Esta regla es NON_COMPLIANT si la versión de metadatos no está incluida en la configuración de lanzamiento o si los metadatos V1 y V2 están habilitados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.10.1	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccess Key La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.
8.3.10.1	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se roten correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.10.1	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.
8.3.11	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.11	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-descanso	Compruebe que haya un grupo de trabajo de Amazon Athena cifrado en reposo. La regla es NON_COMPLIANT si el cifrado de datos en reposo no está habilitado para un grupo de trabajo de Athena.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Compruebe que haya un clúster de base de datos de Amazon Neptune con instantáneas cifradas. La regla es NON_COMPLIANT si un clúster de Neptune no tiene las instantáneas cifradas.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Asegúrese de que los clústeres de Amazon Redshift utilicen una AWS clave específica del Servicio de administración de claves (AWS KMS) para el cifrado. La regla cumple con las normas si el cifrado está activado y el clúster está cifrado con la clave proporcionada en el kmsKeyArn parámetro. La regla es NON_COMPLIANT si el clúster no está cifrado o está cifrado con otra clave.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	codebuild-project-sCifrado de 3 registros	Asegúrese de que un AWS CodeBuild proyecto configura do con Amazon S3 Logs tenga el cifrado activado para sus registros. La regla no es compatible si 'EncryptionDisabled' se establece en 'true' en el S3 LogsConfi g de un proyecto. CodeBuild
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) de los almacenes de datos de Redis estén habilitados para el TLS/SSL cifrado de los datos comunicad os con otros puntos finales. La regla no cumple con los requisitos si el cifrado no está activado. TLS/ SSL

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	eks-secrets-encrypted	Asegúrese de que los clústeres de Amazon Elastic Kubernetes Service estén configurados para cifrar AWS los secretos de Kubernetes mediante claves del Servicio de administración de claves (KMS).
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	api-gw-cache-enabled-y encriptado	Compruebe que todos los métodos de las etapas de Amazon API Gateway tengan memoria caché habilitada y cifrada. La regla es NON_COMPLIANT si algún método de una etapa de Amazon API Gateway no está configurada para el almacenamiento en caché o si la caché no está cifrada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Asegúrese de que la tabla de Amazon DynamoDB esté cifrada AWS con el Servicio de administración de claves (KMS). La regla no es compatible si la tabla de Amazon DynamoDB no está cifrada con KMS. AWS La regla tampoco cumple con los requisitos si la clave de AWS KMS cifrada no está presente en el parámetro de entrada. kmsKeyArns

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-comprobar	Asegúrese de que el proyecto NO contenga variables AWS_ACCESS_KEY_ID de entorno ni _ACCESS_KEY. AWS_SECRET La regla es NON_COMPLIANT si las variables de entorno del proyecto contienen credenciales de texto no cifrado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Asegúrese de que los clústeres de Amazon EKS no estén configurados para cifrar los secretos de Kubernetes mediante KMS. AWS La regla es NON_COMPLIANT si hay un clúster de EKS sin un recurso de encryptionConfig o si encryptionConfig no designa secretos como un recurso.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Compruebe que los flujos de Amazon Kinesis estén cifrados en reposo con el cifrado en el servidor. La regla no cumple con las normas para una transmisión de Kinesis si 'StreamEncryption' no está presente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	msk-in-cluster-node-requerido-tls	Compruebe que haya un clúster de Amazon MSK que aplique el cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Compruebe que el cifrado de almacenamiento esté habilitado para los clústeres de base de datos de Amazon Neptune. La regla es NON_COMPLIANT si el cifrado de almacenamiento no está habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) estén configurados con una conexión SSL. La regla NO ES COMPATIBLE si el AWS DMS no tiene configurada una conexión SSL.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.5	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccess Key La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.
8.3.5	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se roten correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.5	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.
8.3.7	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccessKey La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.7	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se roten correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.
8.3.7	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.9	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccess Key La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.
8.3.9	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se roten correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.9	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.
8.4.1	Se ha implementado la autenticación multifactor (MFA) para proteger el acceso al CDE. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.4.2	Se ha implemento la autenticación multifactor (MFA) para proteger el acceso al CDE. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.
8.4.3	Se ha implemento la autenticación multifactor (MFA) para proteger el acceso al CDE. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.6.3	El uso de las cuentas de aplicación y sistema, y de los factores de autentica ción asociados, se gestiona de forma rigurosa. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccess Key La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.
8.6.3	El uso de las cuentas de aplicación y sistema, y de los factores de autentica ción asociados, se gestiona de forma rigurosa. (PCI-DSS-v4.0)	secretsmanager-sch eduled-rotation-su ccess-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se roten correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.6.3	El uso de las cuentas de aplicación y sistema, y de los factores de autenticación asociados, se gestiona de forma rigurosa. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibido	Compruebe que haya una instantánea manual de un clúster de base de datos de Amazon Neptune que no sea pública. La regla es NON_COMPLIANT si las instantáneas de clústeres nuevas y existentes de Neptune son públicas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no cumple con los requisitos si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING _SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferente s. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario , es NON_COMPL IANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso AWS WAFv2 web ()ACLs. La regla no es compatibl e con una AWS AppSync API si no está asociada a una ACL web.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPL IANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	api-gwv2- access-lo gs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail registro definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimien to que cumpla todos los requisitos siguientes:
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	neptune-cluster-cl oudwatch-log-habil itado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportaci ón de CloudWatc h registros para los registros de auditoría . La regla no es compatible si un clúster de Neptune no tiene habilitad a la exportación de registros para los CloudWatch registros de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla NO ES COMPATIBLE si una ECSTask definició n activa no tiene definido el recurso LogConfiguration o si el valor de LogConfig uration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	appsync-logging-en abled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLog Level» no es ERROR ni ALL.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.3	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	security-account-information-provided	Asegúrese de haber proporcionado la información de contacto de seguridad de los contactos de su AWS cuenta. La regla es NON_COMPLIANT si no se proporcio na la información de contacto de seguridad de la cuenta.
A3.2.5.1	El ámbito del PCI DSS está documenta do y validado. (PCI-DSS-v4.0)	macie-auto-sensitive-data-comprobación-descubrimiento	Compruebe que la detección automatiz ada de datos confidenciales esté habilitada en Amazon Macie. La regla es NON_COMPL IANT si la detección automatizada de datos confidenciales está deshabilitada. La regla es APPLICABL E para las cuentas de administrador y NOT_APPLICABLE para las cuentas de los miembros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.2.5.1	El ámbito del PCI DSS está documentado y validado. (PCI-DSS-v4.0)	macie-status-check	Compruebe que Amazon Macie esté activado en su cuenta por región. La regla es NON_COMPLIANT si el atributo Status no se ha definido como ENABLED.
A3.2.5.2	El ámbito del PCI DSS está documentado y validado. (PCI-DSS-v4.0)	macie-auto-sensitive-data-comprobación-descubrimiento	Compruebe que la detección automatizada de datos confidenciales esté habilitada en Amazon Macie. La regla es NON_COMPLIANT si la detección automatizada de datos confidenciales está deshabilitada. La regla es APPLICABLE para las cuentas de administrador y NOT_APPLICABLE para las cuentas de los miembros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.2.5.2	El ámbito del PCI DSS está documenta do y validado. (PCI-DSS-v4.0)	macie-status-check	Compruebe que Amazon Macie esté activado en su cuenta por región. La regla es NON_COMPLIANT si el atributo Status no se ha definido como ENABLED.
A3.3.1	El PCI DSS está incorporado a las actividades de business-as-usual (BAU). (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
A3.3.1	El PCI DSS está incorporado a las actividades de business-as-usual (BAU). (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
A3.3.1	El PCI DSS está incorporado a las actividades business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan los ajustes especificados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de business-as-usual (BAU). (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.
A3.3.1	El PCI DSS está incorporado a las actividades de business-as-usual (BAU). (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibido	Compruebe que haya una instantánea manual de un clúster de base de datos de Amazon Neptune que no sea pública. La regla es NON_COMPLIANT si las instantáneas de clústeres nuevas y existentes de Neptune son públicas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	backup-recovery-point-manual- eliminación: deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no cumple con los requisitos si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específico de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan la configuración especificada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para PCI DSS 4.0 (excluidos los tipos de recursos globales).

Prácticas operativas recomendadas para el PCI DSS 4.0 (incluye los tipos de recursos globales)

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costos mediante reglas administradas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) 4.0 (excluidos los tipos de recursos globales) y las reglas de AWS Config administradas. Cada AWS Config regla se aplica a un AWS recurso específico y se refiere a uno o más controles de PCI DSS. Un control del PCI DSS puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.5	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	cloudfront-security-policy-check	Asegúrese de que CloudFront las distribuciones de Amazon utilicen una política de seguridad mínima y un conjunto de cifrado de TLSv1 0,2 o superior para las conexiones de los espectado res. Esta regla NO SE AJUSTA a las

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			CloudFront distribuciones si el valor es inferior a .2_2018. minimumProtocolVersion TLSv1
1.2.5	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	cloudfront-sni-enabled	Asegúrese de que CloudFront las distribuciones de Amazon utilicen un certificado SSL personalizado y estén configuradas para utilizar el SNI para atender las solicitudes HTTPS. La regla es NON_COMPLIANT si se asocia un certificado SSL personalizado, pero el método de compatibilidad con SSL es una dirección IP dedicada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.5	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	Asegúrese de que un servidor creado con AWS Transfer Family no utilice FTP para la conexión de punto final. La regla es NON_COMPLIANT si el protocolo del servidor para la conexión del punto de conexión está habilitado para FTP.
1.2.5	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocolos	Asegúrese de que CloudFront las distribuciones no utilicen protocolos SSL obsoletos para la comunicación HTTPS entre ubicaciones de CloudFront borde y orígenes personalizados. Esta regla no cumple con las condiciones de una CloudFront distribución si alguna OriginSslProtocols de ellas «incluye». SSLv3

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.5	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encriptado	Asegúrese de que CloudFron t las distribuc iones de Amazon estén cifrando el tráfico hacia orígenes personali zados. La regla NO CUMPLE CON LOS REQUISITO S si '' es 'solo http' o si '' es 'visor de coincidencias' y OriginProtocolPolicy '' es 'permitido todo'. OriginProtocolPolicy ViewerProtocolPolicy
1.2.5	Los controles de NSCs seguridad de la red () están configura dos y mantenidos. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Asegúrese de que sus CloudFront distribuciones de Amazon utilicen HTTPS (directam ente o mediante una redirección). La regla no cumple con los requisitos si el valor de ViewerPro tocolPolicy está establecido en 'allow-all' para el o para el. DefaultCacheBehavi or CacheBehaviors

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Asegúrese de que CloudFront las distribuciones de Amazon estén asociadas al firewall de aplicaciones web (WAF) o a las listas de control de acceso WAFv2 web (ACLs). La regla no cumple con los requisitos si una CloudFront distribución no está asociada a una ACL web de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFron t distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	rds-db-security-group-no permitido	Compruebe que los grupos de seguridad de base de datos de Amazon Relationa l Database Service (Amazon RDS) sean los predeterm inados. La regla es NON_COMPLIANT si hay algún grupo de seguridad de base de datos que no sea el grupo de seguridad de base de datos predeterminado.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	ec2- -attach-d esactivado transit-g ateway-auto-vpc	Asegúrese de que las pasarelas de tránsito de Amazon Elastic Compute Cloud (Amazon EC2) no tengan " activado. AutoAcceptSharedAt tachments La regla no es conforme para una Transit Gateway si 'AutoAcceptSharedA ttachments' está configurada como 'activa'.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING_SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferentes. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario, es NON_COMPLIANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociados a las listas de control de acceso AWS WAFv2 web (ACLs). La regla no es compatibl e con una AWS AppSync API si no está asociada a una ACL web.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	docdb-cluster-snap shot-public-prohibido	Compruebe que las instantán eas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no cumple con los requisitos si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	waf-global-webacl-not-vacío	Compruebe que haya una ACL web de WAF Global que contenga reglas o grupos de reglas de WAF. Esta regla es NON_COMPLIANT si una ACL web no contiene reglas ni grupos de reglas de WAF.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	waf-global-rule-not-vacío	Asegúrese de que una regla global AWS de WAF contenga algunas condicion es. La regla es NON_COMPLIANT si no hay condiciones presentes en la regla global de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y mantenidos. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.2.8	Los controles de seguridad de la red (NSCs) están configurados y se mantienen. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Asegúrese de que CloudFront las distribuciones de Amazon estén asociadas al firewall de aplicaciones web (WAF) o a las listas de control de acceso WAFv2 web (ACLs). La regla no cumple con los requisitos si una CloudFront distribución no está asociada a una ACL web de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFron t distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	rds-db-security-group-no permitido	Compruebe que los grupos de seguridad de base de datos de Amazon Relationa l Database Service (Amazon RDS) sean los predeterm inados. La regla es NON_COMPLIANT si hay algún grupo de seguridad de base de datos que no sea el grupo de seguridad de base de datos predeterminado.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRoutin g' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	ec2- -attach-desactivado transit-gateway-auto-vpc	Asegúrese de que las pasarelas de tránsito de Amazon Elastic Compute Cloud (Amazon EC2) no tengan " activado. AutoAcceptSharedAttachments La regla no es conforme para una Transit Gateway si 'AutoAcceptSharedAttachments' está configurada como 'activa'.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING _SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferente s. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario , es NON_COMPL IANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso AWS WAFv2 web (). ACLs La regla no es compatibl e con una AWS AppSync API si no está asociada a una ACL web.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	docdb-cluster-snap shot-public-prohibido	Compruebe que las instantán eas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	waf-global-webacl-not-vacío	Compruebe que haya una ACL web de WAF Global que contenga reglas o grupos de reglas de WAF. Esta regla es NON_COMPLIANT si una ACL web no contiene reglas ni grupos de reglas de WAF.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	waf-global-rule-not-vacío	Asegúrese de que una regla global AWS de WAF contenga algunas condicion es. La regla es NON_COMPLIANT si no hay condiciones presentes en la regla global de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.3.1	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Asegúrese de que CloudFront las distribuciones de Amazon estén asociadas al firewall de aplicaciones web (WAF) o a las listas de control de acceso WAFv2 web (ACLs). La regla no cumple con los requisitos si una CloudFront distribución no está asociada a una ACL web de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFron t distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	rds-db-security-group-no permitido	Compruebe que los grupos de seguridad de base de datos de Amazon Relational Database Service (Amazon RDS) sean los predeterminados. La regla es NON_COMPLIANT si hay algún grupo de seguridad de base de datos que no sea el grupo de seguridad de base de datos predeterminado.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRouting' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	ec2- -attach-desactivado transit-gateway-auto-vpc	Asegúrese de que las pasarelas de tránsito de Amazon Elastic Compute Cloud (Amazon EC2) no tengan " activado. AutoAcceptSharedAttachments La regla no es conforme para una Transit Gateway si 'AutoAcceptSharedAttachments' está configurada como 'activa'.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING _SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferente s. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario , es NON_COMPL IANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso AWS WAFv2 web (). ACLs La regla no es compatibl e con una AWS AppSync API si no está asociada a una ACL web.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	docdb-cluster-snap shot-public-prohibido	Compruebe que las instantán eas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	waf-global-webacl-not-vacío	Compruebe que haya una ACL web de WAF Global que contenga reglas o grupos de reglas de WAF. Esta regla es NON_COMPLIANT si una ACL web no contiene reglas ni grupos de reglas de WAF.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	waf-global-rule-not-vacío	Asegúrese de que una regla global AWS de WAF contenga algunas condicion es. La regla es NON_COMPLIANT si no hay condiciones presentes en la regla global de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.3.2	El acceso a la red desde el entorno de datos del titular de la tarjeta, y hacia este, está restringido. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.1	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
1.4.1	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRouting' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.1	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpointConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Asegúrese de que CloudFront las distribuciones de Amazon estén asociadas al firewall de aplicaciones web (WAF) o a las listas de control de acceso WAFv2 web (ACLs). La regla no cumple con los requisitos si una CloudFront distribución no está asociada a una ACL web de WAF.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFron t distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	rds-db-security-group-no permitido	Compruebe que los grupos de seguridad de base de datos de Amazon Relationa l Database Service (Amazon RDS) sean los predeterm inados. La regla es NON_COMPLIANT si hay algún grupo de seguridad de base de datos que no sea el grupo de seguridad de base de datos predeterminado.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRoutin g' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	ec2- -attach-desactivado transit-gateway-auto-vpc	Asegúrese de que las pasarelas de tránsito de Amazon Elastic Compute Cloud (Amazon EC2) no tengan " activado. AutoAcceptSharedAttachments La regla no es conforme para una Transit Gateway si 'AutoAcceptSharedAttachments' está configurada como 'activa'.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING _SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferente s. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario , es NON_COMPL IANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso AWS WAFv2 web (). ACLs La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibido	Compruebe que las instantáneas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	waf-global-webacl-not-vacío	Compruebe que haya una ACL web de WAF Global que contenga reglas o grupos de reglas de WAF. Esta regla es NON_COMPLIANT si una ACL web no contiene reglas ni grupos de reglas de WAF.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	waf-global-rule-not-vacío	Asegúrese de que una regla global AWS de WAF contenga algunas condicion es. La regla es NON_COMPLIANT si no hay condiciones presentes en la regla global de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.4.2	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.3	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.3	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.3	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes completos	Asegúrese de que la política de AWS Network Firewall esté configurada con una acción sin estado predeterminada definida por el usuario para los paquetes completos. La regla es NON_COMPLIANT si la acción predeterminada sin estado para los paquetes completos no coincide con la acción predeterminada sin estado definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.4	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
1.4.4	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-habilitado	Asegúrese de que los clústeres de Amazon Redshift tengan 'enhanced VpcRouting' activado. La regla no cumple con las normas si 'enhancedVpcRoutin g' no está habilitada o si la configuración no está habilitada. enhancedVpcRouting el campo es «falso».

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.4	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.
1.4.5	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	ecs-task-definition-pid-comprobación de modo	Asegúrese de que ECSTask las definiciones estén configuradas para compartir el espacio de nombres de procesos de un host con sus contenedores de Amazon Elastic Container Service (Amazon ECS). La regla es NON_COMPLIANT si el parámetro pidMode está establecido en “host”.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.4.5	Las conexiones de red entre redes confiables y no confiables están controladas. (PCI-DSS-v4.0)	ec2- -deshabilitado launch-template-public-ip	Compruebe que las plantillas de lanzamiento de Amazon EC2 no estén configuradas para asignar direcciones IP públicas a interfaces de red. La regla no cumple con los requisitos si la versión predeterminada de una plantilla de lanzamiento de EC2 tiene al menos una interfaz de red con el valor «verdadero». AssociatePublicIpAddress

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpointConfigurationType'. La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Asegúrese de que CloudFront las distribuciones de Amazon estén asociadas al firewall de aplicaciones web (WAF) o a las listas de control de acceso WAFv2 web (ACLs). La regla no cumple con los requisitos si una CloudFront distribución no está asociada a una ACL web de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmentados. La regla es NON_COMPLIANT si la acción predeterminada sin estado para los paquetes fragmentados no coincide con la acción predeterminada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	rds-db-security-group-no permitido	Compruebe que los grupos de seguridad de base de datos de Amazon Relational Database Service (Amazon RDS) sean los predeterminados. La regla es NON_COMPLIANT si hay algún grupo de seguridad de base de datos que no sea el grupo de seguridad de base de datos predeterminado.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	ec2- -attach-desactivado transit-gateway-auto-vpc	Asegúrese de que las pasarelas de tránsito de Amazon Elastic Compute Cloud (Amazon EC2) no tengan " activado. AutoAcceptSharedAttachments La regla no es conforme para una Transit Gateway si 'AutoAcceptSharedAttachments' está configurada como 'activa'.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING_SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferentes. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario, es NON_COMPLIANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso AWS WAFv2 web (). ACLs La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibido	Compruebe que las instantáneas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	waf-global-webacl-not-vacío	Compruebe que haya una ACL web de WAF Global que contenga reglas o grupos de reglas de WAF. Esta regla es NON_COMPLIANT si una ACL web no contiene reglas ni grupos de reglas de WAF.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	waf-global-rule-not-vacío	Asegúrese de que una regla global AWS de WAF contenga algunas condiciones. La regla es NON_COMPLIANT si no hay condiciones presentes en la regla global de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
1.5.1	Se han mitigado los riesgos para el CDE desde dispositivos de computación con capacidad de conexión al CDE y a redes no confiables. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definicio nes de tareas de Amazon ECS. Esta regla no es compatibl e si una ECSTask definición activa no tiene definido el recurso LogConfig uration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web ACLs). La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitado para todos los tipos de registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs
10.2.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitado la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
102.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definicio nes de tareas de Amazon ECS. Esta regla no es compatibl e si una ECSTask definición activa no tiene definido el recurso LogConfig uration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web). ACLs La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitado para todos los tipos de registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
102.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs
10.2.1.1	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsE nabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.
102.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.1	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web). ACLs La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.2.1.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitado para todos los tipos de registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-lo gs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web). ACLs La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.2.1.3	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitado para todos los tipos de registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.3	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-lo gs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web). ACLs La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.2.1.4	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.4	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web). ACLs La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.2.1.5	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitado para todos los tipos de registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.5	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.
10.2.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-lo gs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web). ACLs La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.2.1.6	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitado para todos los tipos de registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
102.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs
10.2.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.6	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.
10.2.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-lo gs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web). ACLs La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitado para todos los tipos de registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
102.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs
10.2.1.7	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.1.7	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web ACLs). La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.2.2	Se han implemento registros de auditoría como apoyo para la detección de anomalías y actividades sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitado para todos los tipos de registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs
10.2.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.2.2	Se han implement ado registros de auditoría como apoyo para la detección de anomalías y actividad es sospechosas, así como para el análisis forense de los eventos. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	api-gwv2- access-lo gs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración de Stage.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla no es compatible si una ECSTask definición activa no tiene definido el recurso LogConfiguration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TRAIL_ENABLED) y el nombre de la regla (cloudtrail-enabled) son diferentes. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimiento habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLog Level» no es ERROR ni ALL.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web ACLs). La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.3.1	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimien to que cumpla todos los requisitos siguientes:
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibido	Compruebe que haya una instantán ea manual de un clúster de base de datos de Amazon Neptune que no sea pública. La regla es NON_COMPLIANT si las instantáneas de clústeres nuevas y existentes de Neptune son públicas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibido	Compruebe que las instantáneas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla es NON_COMPLIANT si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.
10.3.2	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	aurora-resources-protected-by-plan de respaldo	Compruebe que los clústeres de bases de datos de Amazon Aurora estén protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el clúster de bases de datos de Amazon Relational Database Service (Amazon RDS) no está protegido por un plan de copia de seguridad.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	db-instance-backup-enabled	Compruebe que las instancias de base de datos de RDS tengan habilitada la copia de seguridad. Opcionalmente, la regla comprueba el periodo de retención de copia de seguridad y el periodo de tiempo de la copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	dynamodb-in-backup-plan	Asegúrese de que las tablas de Amazon DynamoDB estén presentes en AWS los planes de Backup. La regla no es conforme si las tablas de Amazon DynamoDB no están presentes en ningún plan de Backup. AWS
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	dynamodb-resources-protected-by-plan de respaldo	Compruebe que las tablas de Amazon DynamoDB estén protegidas por un plan de copia de seguridad. La regla es NON_COMPLIANT si la tabla de DynamoDB no está cubierta por un plan de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	ebs-in-backup-plan	Asegúrese de añadir los volúmenes de Amazon Elastic Block Store (Amazon EBS) a los planes de backup de Backup. AWS La regla es NON_COMPLIANT si los volúmenes de Amazon EBS no están incluidos en los planes de copia de seguridad.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	ebs-resources-protected-by-plan de respaldo	Compruebe que los volúmenes de Amazon Elastic Block Store (Amazon EBS) estén protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el volumen de Amazon EBS no está cubierto por un plan de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	ec2- -plan resources-protected-by-backup	Compruebe que las instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén protegidas por un plan de copia de seguridad. La regla es NON_COMPLIANT si la instancia de Amazon EC2 no está cubierta por un plan de copia de seguridad .
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	efs-in-backup-plan	Asegúrese de añadir los sistemas de archivos Amazon Elastic File System (Amazon EFS) a los planes de AWS backup de Backup. La regla es NON_COMPLIANT si los sistemas de archivos de EFS no están incluidos en los planes de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	efs-resources-protected-by-plan de respaldo	Compruebe que los sistemas de archivos de Amazon Elastic File System (Amazon EFS) estén protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el sistema de archivos de EFS no está cubierto por un plan de copia de seguridad.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	elasticache-redis-cluster-automatic-verificación de respaldo	Compruebe si los clústeres de Amazon ElastiCache Redis tienen activada la copia de seguridad automática. La regla no es compatible si el clúster SnapshotRetentionLimit de Redis es inferior al parámetro. SnapshotRetentionPeriod Por ejemplo: si el parámetro es 15, la regla no es compatible si está entre 0 y 15. snapshotRetentionPeriod

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	fsx-resources-protected-by-plan de respaldo	Asegúrese de que Amazon FSx File Systems esté protegido por un plan de respaldo. La regla no cumple con los requisitos si el sistema de FSx archivos de Amazon no está cubierto por un plan de respaldo.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	neptune-cluster-backup-retention-comprobar	Compruebe que el período de retención de un clúster de base de datos de Amazon Neptune se haya configurado a un número específico o de días. La regla es NON_COMPLIANT si el período de retención es inferior al valor especificado por el parámetro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	rds-in-backup-plan	Asegúrese de que las bases de datos de Amazon Relational Database Service (Amazon RDS) estén presentes en los planes de AWS Backup. La regla no es conforme si las bases de datos de Amazon RDS no están incluidas en ningún plan de Backup AWS .
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	rds-resources-protected-by-plan de respaldo	Compruebe que las instancias de Amazon Relational Database Service (Amazon RDS) estén protegidas por un plan de copia de seguridad. La regla es NON_COMPLIANT si la instancia de Amazon RDS no está cubierta por un plan de copia de seguridad .

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	redshift-backup-enabled	Compruebe que las instantáneas automatizadas de Amazon Redshift estén habilitadas para clústeres. La regla no es compatible si el valor del automated SnapshotRetention período es mayor MaxRetentionPeriod o menor que MinRetentionPeriod o el valor es 0.
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	plan s3 resources-protected-by-backup	Compruebe que los buckets de Amazon Simple Storage Service (Amazon S3) estén protegidos por un plan de copia de seguridad. La regla es NON_COMPLIANT si el bucket de Amazon S3 no está cubierto por un plan de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimien to que cumpla todos los requisitos siguientes:
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	db-instance-backup-enabled	Compruebe que las instancias de base de datos de RDS tengan habilitada la copia de seguridad . Opcionalmente, la regla comprueba el periodo de retención de copia de seguridad y el periodo de tiempo de la copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.3	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.
10.3.4	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudfront-origin-access-identity-habilitado	Asegúrese de que CloudFront la distribución con el tipo de origen Amazon S3 tenga configurada la identidad de acceso de origen (OAI). La regla no es compatible si la CloudFront distribución está respaldada por S3 y cualquier tipo de origen no está configurado con OAI o si el origen no es un bucket de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.4	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	frente a nubos-s3-origin-access-control-enabled	Asegúrese de que una CloudFron t distribución de Amazon con un tipo de origen Amazon Simple Storage Service (Amazon S3) tenga activado el control de acceso de origen (OAC). La regla es NON_COMPLIANT para CloudFront las distribuciones con orígenes de Amazon S3 que no tienen habilitada la OAC.
10.3.4	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	s3- bucket-default-loc k-enabled	Compruebe que el bucket de S3 tenga habilitado el bloqueo de forma predeterm inada. La regla es NON_COMPLIANT si el bloqueo no está habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.3.4	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	s3- bucket-versioning-enabled	Compruebe que se haya habilitado el control de versiones para los buckets de S3. Opcionalmente, la regla comprueba si la eliminación de MFA está habilitada para los buckets de S3.
10.3.4	Los registros de auditoría están protegidos frente a la destrucción y las modificaciones no autorizadas. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimien to que cumpla todos los requisitos siguientes:
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICI ENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especific ado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-r esource-check	Asegúrese de que un tipo de recurso tenga una CloudWatc h alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsE nabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-r esource-check	Asegúrese de que un tipo de recurso tenga una CloudWatc h alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsE nabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.1.1	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especific ado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-r esource-check	Asegúrese de que un tipo de recurso tenga una CloudWatc h alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsE nabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.2	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.4.3	Se revisan los registros de auditoría para identificar anomalías o actividad es sospechosas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimiento que cumpla todos los requisitos siguientes:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPLIANT si PITR no está habilitado para las tablas de DynamoDB.
10.5.1	Se conserva un historial del registro de auditoría y está disponible para el análisis. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-habilitado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportación de CloudWatch registros para los registros de auditoría. La regla no es compatible si un clúster de Neptune no tiene habilitada la exportación de registros para los CloudWatch registros de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definicio nes de tareas de Amazon ECS. Esta regla no es compatibl e si una ECSTask definición activa no tiene definido el recurso LogConfig uration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TRAIL_ENABLED) y el nombre de la regla (cloudtrail-enabled) son diferentes. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimiento habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLog Level» no es ERROR ni ALL.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web ACLs). La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
10.6.3	Los mecanismos de sincronización horaria permiten que la configuración horaria sea uniforme en todos los sistemas. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Asegúrate de que tus CloudForm ation stacks envíen notificaciones de eventos a un tema de Amazon SNS. Como caracterí stica opcional, compruebe que se estén utilizando los temas de Amazon SNS especificados. La regla no cumple con los requisitos si las CloudForm ation pilas no envían notificaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.1	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Asegúrate de que tus CloudFormation stacks envíen notificaciones de eventos a un tema de Amazon SNS. Como característica opcional, compruebe que se estén utilizando los temas de Amazon SNS especificados. La regla no cumple con los requisitos si las CloudFormation pilas no envían notificaciones.
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitado la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
10.7.2	Los fallos de los sistemas de control de seguridad críticos se detectan y se notifican, y se responde a ellos con prontitud. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.5.2	Las intrusiones en la red y los cambios inesperados en los archivos se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Asegúrate de que tus CloudFormation stacks envíen notificaciones de eventos a un tema de Amazon SNS. Como característica opcional, compruebe que se estén utilizando los temas de Amazon SNS especificados. La regla no cumple con los requisitos si las CloudFormation pilas no envían notificaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.5.2	Las intrusiones en la red y los cambios inesperados en los archivos se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.5.2	Las intrusiones en la red y los cambios inesperados en los archivos se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.
11.5.2	Las intrusiones en la red y los cambios inesperados en los archivos se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan la configuración especificada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.5.2	Las intrusiones en la red y los cambios inesperados en los archivos se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.6.1	Los cambios no autorizados en las páginas de pago se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Asegúrate de que tus CloudFormation stacks envíen notificaciones de eventos a un tema de Amazon SNS. Como característica opcional, compruebe que se estén utilizando los temas de Amazon SNS especificados. La regla no cumple con los requisitos si las CloudFormation pilas no envían notificaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.6.1	Los cambios no autorizados en las páginas de pago se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.6.1	Los cambios no autorizados en las páginas de pago se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.
11.6.1	Los cambios no autorizados en las páginas de pago se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan la configuración especificada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
11.6.1	Los cambios no autorizados en las páginas de pago se detectan y se proporciona una respuesta. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.10.5	Se responde inmediatamente a los incidentes de seguridad, sospechosos y confirmados, que puedan afectar al CDE. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Asegúrate de que tus CloudFormation stacks envíen notificaciones de eventos a un tema de Amazon SNS. Como característica opcional, compruebe que se estén utilizando los temas de Amazon SNS especificados. La regla no cumple con los requisitos si las CloudFormation pilas no envían notificaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.10.5	Se responde inmediatamente a los incidentes de seguridad, sospechosos y confirmados, que puedan afectar al CDE. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.10.5	Se responde inmediatamente a los incidentes de seguridad, sospechosos y confirmados, que puedan afectar al CDE. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.
12.10.5	Se responde inmediatamente a los incidentes de seguridad, sospechosos y confirmados, que puedan afectar al CDE. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan la configuración especificada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
12.10.5	Se responde inmediatamente a los incidentes de seguridad, sospechosos y confirmados, que puedan afectar al CDE. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.
12.4.2.1	El cumplimiento de PCI DSS está administrado. (PCI-DSS-v4.0)	service-catalog-shared-within-organización	Asegúrese de que AWS Service Catalog comparta las carteras con una organización (un conjunto de AWS cuentas tratadas como una sola unidad) cuando la integración esté habilitada con AWS Organizations. La regla es NON_COMPLIANT si el valor de Tipo al compartir es ACCOUNT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.5	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	cloudfront-security-policy-check	Asegúrese de que CloudFront las distribuciones de Amazon utilicen una política de seguridad mínima y un conjunto de cifrado de TLSv1 0,2 o superior para las conexiones de los espectado res. Esta regla NO SE AJUSTA a las CloudFront distribuc iones si el valor es inferior a .2_2018. minimumProtocolVer sion TLSv1

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.5	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	cloudfront-sni-enabled	Asegúrese de que CloudFront las distribuciones de Amazon utilicen un certificado SSL personalizado y estén configuradas para utilizar el SNI para atender las solicitudes HTTPS. La regla es NON_COMPLIANT si se asocia un certifica do SSL personali zado, pero el método de compatibilidad con SSL es una dirección IP dedicada.
2.2.5	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	Asegúrese de que un servidor creado con AWS Transfer Family no utilice FTP para la conexión de punto final. La regla es NON_COMPL IANT si el protocolo del servidor para la conexión del punto de conexión está habilitado para FTP.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.5	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	cloudfront-no-depr ecated-ssl-protocolos	Asegúrese de que CloudFront las distribuciones no utilicen protocolos SSL obsoletos para la comunicación HTTPS entre ubicaciones de CloudFront borde y orígenes personali zados. Esta regla no cumple con las condiciones de una CloudFront distribuc ión si alguna OriginSsl Protocols de ellas «incluye». SSLv3

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.5	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encriptado	Asegúrese de que CloudFron t las distribuc iones de Amazon estén cifrando el tráfico hacia orígenes personali zados. La regla NO CUMPLE CON LOS REQUISITO S si '' es 'solo http' o si '' es 'visor de coincidencias' y OriginProtocolPolicy '' es 'permitido todo'. OriginProtocolPolicy ViewerProtocolPolicy
2.2.5	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Asegúrese de que sus CloudFront distribuciones de Amazon utilicen HTTPS (directam ente o mediante una redirección). La regla no cumple con los requisitos si el valor de ViewerPro tocolPolicy está establecido en 'allow-all' para el o para el. DefaultCacheBehavi or CacheBehaviors

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) de los almacenes de datos de Redis estén habilitados para el TLS/SSL cifrado de los datos comunicad os con otros puntos finales. La regla no cumple con los requisitos si el cifrado no está activado. TLS/SSL
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	cloudfront-no-depr ecated-ssl-protocolos	Asegúrese de que CloudFront las distribuciones no utilicen protocolos SSL obsoletos para la comunicación HTTPS entre ubicaciones de CloudFront borde y orígenes personali zados. Esta regla no cumple con las condiciones de una CloudFront distribuc ión si alguna OriginSsl Protocols de ellas «incluye». SSLv3

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encriptado	Asegúrese de que CloudFron t las distribuc iones de Amazon estén cifrando el tráfico hacia orígenes personali zados. La regla NO CUMPLE CON LOS REQUISITO S si '' es 'solo http' o si '' es 'visor de coincidencias' y OriginProtocolPolicy '' es 'permitido todo'. OriginProtocolPolicy ViewerProtocolPolicy
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Asegúrese de que sus CloudFront distribuciones de Amazon utilicen HTTPS (directam ente o mediante una redirección). La regla no cumple con los requisitos si el valor de ViewerPro tocolPolicy está establecido en 'allow-all' para el o para el. DefaultCacheBehavi or CacheBehaviors

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.7	Los componentes del sistema se configuran y administran de forma segura. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Asegúrese de que su clúster de Amazon DynamoDB Accelerator (DAX) esté configurado en TLS. ClusterEndpointEncryptionType La regla es NON_COMPLIANT si hay un clúster de DAX que no está cifrado con seguridad de la capa de transporte (TLS).
2.2.7	Los componentes del sistema se configuran y administran de forma segura. (PCI-DSS-v4.0)	msk-in-cluster-node-requerido-tls	Compruebe que haya un clúster de Amazon MSK que aplique el cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
2.2.7	Los componentes del sistema se configura n y administran de forma segura. (PCI-DSS-v4.0)	dms-endpoint-ssl-c onfigured	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) estén configurados con una conexión SSL. La regla NO ES COMPATIBLE si el AWS DMS no tiene configurada una conexión SSL.
3.2.1	El almacenamiento de los datos de la cuenta se reduce al mínimo. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1	El almacenamiento de los datos de la cuenta se reduce al mínimo. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.
3.2.1	El almacenamiento de los datos de la cuenta se reduce al mínimo. (PCI-DSS-v4.0)	dynamodb-pitr-enab led	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPL IANT si PITR no está habilitado para las tablas de DynamoDB.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.2.1	El almacenamiento de los datos de la cuenta se reduce al mínimo. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.
3.3.1.1	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1.1	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.
3.3.1.1	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPL IANT si PITR no está habilitado para las tablas de DynamoDB.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1.1	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.
3.3.1.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.
3.3.1.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPL IANT si PITR no está habilitado para las tablas de DynamoDB.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.1.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.
3.3.2	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.
3.3.2	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPL IANT si PITR no está habilitado para las tablas de DynamoDB.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.2	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.
3.3.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ec-2 volume-inuse-check	Compruebe que los volúmenes de EBS estén asociados a instancias de EC2. Como factor opcional, compruebe que los volúmenes de EBS se marquen para eliminarlos cuando se finaliza una instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configurado	Compruebe que haya un repositorio privado de Amazon Elastic Container Registry (ECR) con, al menos, una política de ciclo de vida configurada. La regla es NON_COMPLIANT si no se ha configura do ninguna política de ciclo de vida para el repositorio privado de ECR.
3.3.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Asegúrese de que point-in-time la recuperación (PITR) esté habilitada para las tablas de Amazon DynamoDB. La regla es NON_COMPL IANT si PITR no está habilitado para las tablas de DynamoDB.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3.3	Los datos de autenticación confidenciales (SAD) no se almacenan después de la autorización. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-descanso	Compruebe que haya un grupo de trabajo de Amazon Athena cifrado en reposo. La regla es NON_COMPLIANT si el cifrado de datos en reposo no está habilitado para un grupo de trabajo de Athena.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Compruebe que haya un clúster de base de datos de Amazon Neptune con instantáneas cifradas. La regla es NON_COMPLIANT si un clúster de Neptune no tiene las instantáneas cifradas.
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Asegúrese de que los clústeres de Amazon Redshift utilicen una AWS clave específica del Servicio de administración de claves (AWS KMS) para el cifrado. La regla cumple con las normas si el cifrado está activado y el clúster está cifrado con la clave proporcionada en el kmsKeyArn parámetro. La regla es NON_COMPLIANT si el clúster no está cifrado o está cifrado con otra clave.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	codebuild-project-artifact-encryption	Asegúrese de que un AWS CodeBuild proyecto tenga activado el cifrado de todos sus artefactos. La regla kms:DescribeKey si encryptionDisabled se establece en true para cualquier configuración de artefacto principal o secundario (si está presente).
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	codebuild-project-sCifrado de 3 registros	Asegúrese de que un AWS CodeBuild proyecto configurado con Amazon S3 Logs tenga el cifrado activado para sus registros. La regla no cumple con los requisitos si «EncryptionDisabled» se establece en «verdadero» en el S3 de un proyecto. LogsConfig CodeBuild

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	dax-encryption-enabled	Compruebe que los clústeres del Acelerador de Amazon DynamoDB (DAX) estén cifrados. La regla es NON_COMPLIANT si el clúster de DAX no está cifrado.
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	eks-secrets-encrypted	Asegúrese de que los clústeres de Amazon Elastic Kubernetes Service estén configurados para cifrar AWS los secretos de Kubernetes mediante claves del Servicio de administración de claves (KMS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	api-gw-cache-enabled-y encriptado	Compruebe que todos los métodos de las etapas de Amazon API Gateway tengan memoria caché habilitada y cifrada. La regla es NON_COMPLIANT si algún método de una etapa de Amazon API Gateway no está configurada para el almacenamiento en caché o si la caché no está cifrada.
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	docdb-cluster-encrypted	Compruebe que el cifrado de almacenamiento esté habilitado en los clústeres de Amazon DocumentDB (compatible con MongoDB). La regla es NON_COMPLIANT si el cifrado de almacenamiento no está habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Asegúrese de que la tabla de Amazon DynamoDB esté cifrada AWS con el Servicio de administración de claves (KMS). La regla no es compatible si la tabla de Amazon DynamoDB no está cifrada con KMS. AWS La regla tampoco cumple con los requisitos si la clave de AWS KMS cifrada no está presente en el parámetro de entrada. kmsKeyArns
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	dynamodb-table-encryption-enabled	Compruebe que las tablas de Amazon DynamoDB estén cifradas y revise su estado. La regla es COMPLIANT si el estado indica que se han habilitado o se están habilitando.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-comprobar	Asegúrese de que el proyecto NO contenga variables de entorno ni AWS_ACCESS_KEY_ID AWS_SECRET _ACCESS_KEY. La regla es NON_COMPLIANT si las variables de entorno del proyecto contienen credenciales de texto no cifrado.
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Asegúrese de que los clústeres de Amazon EKS no estén configurados para cifrar los secretos de Kubernetes mediante KMS. AWS La regla es NON_COMPLIANT si hay un clúster de EKS sin un recurso de encryptionConfig o si encryptionConfig no designa secretos como un recurso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Compruebe que los flujos de Amazon Kinesis estén cifrados en reposo con el cifrado en el servidor. La regla no es conforme para una transmisión de Kinesis si 'StreamEncryption' no está presente.
3.5.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Compruebe que el cifrado de almacenamiento esté habilitado para los clústeres de base de datos de Amazon Neptune. La regla es NON_COMPLIANT si el cifrado de almacenamiento no está habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.5.1.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.1	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFron t distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibido	Compruebe que haya una instantán ea manual de un clúster de base de datos de Amazon Neptune que no sea pública. La regla es NON_COMPLIANT si las instantáneas de clústeres nuevas y existentes de Neptune son públicas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibido	Compruebe que las instantáneas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla es NON_COMPLIANT si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen puertos distintos del puerto 22. PermittedPublicSecurityGroupRuleRanges
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.
3.5.1.3	El número de cuenta principal (PAN) está protegido dondequiera que esté almacenado. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.6.1	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.
3.6.1.2	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1.2	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
3.6.1.2	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1.3	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.6.1.3	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1.3	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.
3.6.1.4	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.6.1.4	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
3.6.1.4	Las claves criptográficas utilizadas para proteger los datos de cuenta almacenados están protegidas. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.1	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-certificate-rsa-check	Asegúrese de que los certificados RSA administrados por AWS Certificate Manager (ACM) tengan una longitud de clave de al menos «2048» bits. La regla no es compatible si la longitud mínima de la clave es inferior a 2048 bits.
3.7.1	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS privada (CA AWS privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.1	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.1	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.2	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.7.2	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.2	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.4	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.7.4	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.4	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.6	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.7.6	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.6	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.7	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.
3.7.7	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.7.7	Cuando se utiliza la criptografía para proteger los datos de cuenta almacenados, se definen e implementan procesos y procedimientos de administración de claves que abarcan todos los aspectos del ciclo de vida de las claves. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) de los almacenes de datos de Redis estén habilitados para el TLS/SSL cifrado de los datos comunicados con otros puntos finales. La regla no cumple con los requisitos si el cifrado no está activado. TLS/SSL
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocolos	Asegúrese de que CloudFront las distribuciones no utilicen protocolos SSL obsoletos para la comunicación HTTPS entre ubicaciones de CloudFront borde y orígenes personalizados. Esta regla no cumple con las condiciones de una CloudFront distribución si alguna OriginSslProtocols de ellas «incluye». SSLv3

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encriptado	Asegúrese de que CloudFront las distribuciones de Amazon estén cifrando el tráfico hacia orígenes personalizados. La regla NO CUMPLE CON LOS REQUISITOS si '' es 'solo http' o si '' es 'visor de coincidencias' y OriginProtocolPolicy '' es 'permitido todo'. OriginProtocolPolicy ViewerProtocolPolicy
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Asegúrese de que sus CloudFront distribuciones de Amazon utilicen HTTPS (directamente o mediante una redirección). La regla no cumple con los requisitos si el valor de ViewerProtocolPolicy está establecido en 'allow-all' para el o para el. DefaultCacheBehavior CacheBehaviors

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Asegúrese de que su clúster de Amazon DynamoDB Accelerator (DAX) esté configurado en TLS. ClusterEndpointEncryptionType La regla es NON_COMPLIANT si hay un clúster de DAX que no está cifrado con seguridad de la capa de transporte (TLS).
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	msk-in-cluster-node-requerido-tls	Compruebe que haya un clúster de Amazon MSK que aplique el cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) estén configurados con una conexión SSL. La regla NO ES COMPATIBLE si el AWS DMS no tiene configurada una conexión SSL.
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	acm-pca-root-ca-deshabilitado	Asegúrese de que la autoridad de certificación AWS AWS privada (CA privada) tenga una CA raíz deshabilitada. La regla no cumple con los requisitos para la raíz CAs con un estado que no esté DESHABILITADO.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFront distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) de los almacenes de datos de Redis estén habilitados para el TLS/SSL cifrado de los datos comunicados con otros puntos finales. La regla no cumple con los requisitos si el cifrado no está activado. TLS/SSL

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocolos	Asegúrese de que CloudFront las distribuciones no utilicen protocolos SSL obsoletos para la comunicación HTTPS entre ubicaciones de CloudFront borde y orígenes personalizados. Esta regla no cumple con las condiciones de una CloudFront distribución si alguna OriginSslProtocols de ellas «incluye». SSLv3

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encriptado	Asegúrese de que CloudFront las distribuciones de Amazon estén cifrando el tráfico hacia orígenes personalizados. La regla NO CUMPLE CON LOS REQUISITOS si '' es 'solo http' o si '' es 'visor de coincidencias' y OriginProtocolPolicy '' es 'permitido todo'. OriginProtocolPolicy ViewerProtocolPolicy
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Asegúrese de que sus CloudFront distribuciones de Amazon utilicen HTTPS (directamente o mediante una redirección). La regla no cumple con los requisitos si el valor de ViewerProtocolPolicy está establecido en 'allow-all' para el o para el. DefaultCacheBehavior CacheBehaviors

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Asegúrese de que su clúster de Amazon DynamoDB Accelerator (DAX) esté configurado en TLS. ClusterEndpointEncryptionType La regla es NON_COMPLIANT si hay un clúster de DAX que no está cifrado con seguridad de la capa de transporte (TLS).
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	msk-in-cluster-node-requerido-tls	Compruebe que haya un clúster de Amazon MSK que aplique el cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.2.1.1	Durante la transmisión, el PAN está protegido con un potente método criptográfico. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) estén configurados con una conexión SSL. La regla NO ES COMPATIBLE si el AWS DMS no tiene configurada una conexión SSL.
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitado el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribución no tiene el registro configurado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail sendero definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimien to que cumpla todos los requisitos siguientes:
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	neptune-cluster-cl oudwatch-log-habil itado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportaci ón de CloudWatc h registros para los registros de auditoría . La regla no es compatible si un clúster de Neptune no tiene habilitad a la exportación de registros para los CloudWatch registros de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definicio nes de tareas de Amazon ECS. Esta regla no es compatibl e si una ECSTask definición activa no tiene definido el recurso LogConfig uration o si el valor de LogConfiguration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TRAIL_ENABLED) y el nombre de la regla (cloudtrail-enabled) son diferentes. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su AWS cuenta. La regla es NON_COMPLIANT si no hay ningún registro de seguimiento habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_REGION_CLOUD_TRAIL_ENABLED) y el nombre de la regla () son diferentes. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPLIANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPLIANT si el ExcludeManagementEventSources campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	appsync-logging-enabled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLogLevel» no es ERROR ni ALL.
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitado en las listas de control de acceso web globales clásicas de AWS WAF (web ACLs). La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
5.3.4	Los mecanismos y procesos antimalwa re están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
5.3.4	Los mecanismos y procesos antimalware están activos, supervisados y bajo mantenimiento. (PCI-DSS-v4.0)	cw-loggroup-retention-period-comprobar	Asegúrese de que el período CloudWatch LogGroup de retención de Amazon sea superior a 365 días o, de lo contrario, un período de retención específico. La regla NO CUMPLE CON LOS REQUISITOS si el período de retención es inferior a MinRetentionTime, si se especifica, o bien 365 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3.3	Las vulnerabilidades de seguridad se identifican y se gestionan. (PCI-DSS-v4.0)	lambda-function-settings-check	Asegúrese de que la configuración de la función AWS Lambda para el tiempo de ejecución , la función, el tiempo de espera y el tamaño de la memoria coincidan con los valores esperados . La regla ignora las funciones con el tipo de paquete “Image” y las funciones con el tiempo de ejecución establecido en Tiempo de ejecución exclusivo del sistema operativo. La regla es NON_COMPLIANT si la configuración de la función de Lambda no coincide con los valores esperados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3.3	Las vulnerabilidades de seguridad se identifican y se gestionan. (PCI-DSS-v4.0)	eks-cluster-oldest-supported-versión	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (EKS) que no ejecute la versión compatible más antigua. La regla es NON_COMPL IANT si un clúster de EKS ejecuta la versión compatible más antigua (igual al parámetro oldestVer sionSupported).
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Asegúrese de que CloudFront las distribuciones de Amazon estén asociadas al firewall de aplicaciones web (WAF) o a las listas de control de acceso WAFv2 web (ACLs). La regla no cumple con los requisitos si una CloudFront distribución no está asociada a una ACL web de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso a la AWS WAFv2 web (ACLs). La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	guerra 2- webacl-not-empty	Asegúrese de que una ACL WAFv2 web contenga cualquier regla de WAF o grupo de reglas de WAF. Esta regla NON_COMPLIANT si una ACL web no contiene reglas de WAF ni grupos de reglas de WAF.
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	guerra 2- rulegroup-not-empty	Asegúrese de que los WAFv2 grupos de reglas contengan reglas. La regla no es compatible si no hay reglas en un WAFv2 grupo de reglas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	waf-global-webacl-not-vacío	Compruebe que haya una ACL web de WAF Global que contenga reglas o grupos de reglas de WAF. Esta regla es NON_COMPLIANT si una ACL web no contiene reglas ni grupos de reglas de WAF.
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4.1	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	waf-global-rule-not-vacío	Asegúrese de que una regla global AWS de la WAF contenga algunas condiciones. La regla es NON_COMPLIANT si no hay condiciones presentes en la regla global de WAF.
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Asegúrese de que CloudFront las distribuciones de Amazon estén asociadas al firewall de aplicaciones web (WAF) o a las listas de control de acceso WAFv2 web (ACLs). La regla no cumple con los requisitos si una CloudFront distribución no está asociada a una ACL web de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso a la AWS WAFv2 web (ACLs). La regla no es compatible con una AWS AppSync API si no está asociada a una ACL web.
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	guerra 2- webacl-not-empty	Asegúrese de que una ACL WAFv2 web contenga cualquier regla de WAF o grupo de reglas de WAF. Esta regla NON_COMPLIANT si una ACL web no contiene reglas de WAF ni grupos de reglas de WAF.
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	guerra 2- rulegroup-not-empty	Asegúrese de que los WAFv2 grupos de reglas contengan reglas. La regla no es compatible si no hay reglas en un WAFv2 grupo de reglas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	waf-global-webacl-not-vacío	Compruebe que haya una ACL web de WAF Global que contenga reglas o grupos de reglas de WAF. Esta regla es NON_COMPLIANT si una ACL web no contiene reglas ni grupos de reglas de WAF.
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.4.2	Las aplicaciones web orientadas al público están protegidas frente a ataques. (PCI-DSS-v4.0)	waf-global-rule-not-vacío	Asegúrese de que una regla global AWS de la WAF contenga algunas condiciones. La regla es NON_COMPLIANT si no hay condiciones presentes en la regla global de WAF.
6.5.5	Los cambios en todos los componentes del sistema se administr an de forma segura. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-turno desactivado	Compruebe que el grupo de implement ación de la plataform a de computación Lambda no utilice la configuración de implementación predeterminada. La regla no es compatibl e si el grupo de despliegue utiliza la configuración de despliegue '. CodeDeployDefault LambdaAllAtOnce'.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.5.5	Los cambios en todos los componentes del sistema se administr an de forma segura. (PCI-DSS-v4.0)	codepipeline-deplo yment-count-check	Asegúrese de que en la primera etapa de despliegue se AWS CodePipeline realice al menos un despliegue. Esto permite supervisar la actividad continua de implementación para garantizar que haya actualiza ciones periódicas y para identificar las canalizaciones inactivas o infrautil izadas, lo que puede indicar la existencia de problemas en el proceso de desarroll o o implementación. Como característica opcional, compruebe que todas las etapas restantes posterior es se implement en en un número mayor al especificado (deploymentLimit).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.5.6	Los cambios en todos los componentes del sistema se administr an de forma segura. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-turno desactivado	Compruebe que el grupo de implement ación de la plataform a de computación Lambda no utilice la configuración de implementación predeterminada. La regla no es compatibl e si el grupo de despliegue utiliza la configuración de despliegue '. CodeDeployDefault LambdaAllAtOnce'.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.5.6	Los cambios en todos los componentes del sistema se administr an de forma segura. (PCI-DSS-v4.0)	codepipeline-deplo yment-count-check	Asegúrese de que en la primera etapa de despliegue se AWS CodePipeline realice al menos un despliegue. Esto permite supervisar la actividad continua de implementación para garantizar que haya actualiza ciones periódicas y para identificar las canalizaciones inactivas o infrautil izadas, lo que puede indicar la existencia de problemas en el proceso de desarroll o o implementación. Como característica opcional, compruebe que todas las etapas restantes posterior es se implement en en un número mayor al especificado (deploymentLimit).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	shield-drt-access	Asegúrese de que el Shield Response Team (SRT) pueda acceder a su AWS cuenta. La regla es NON_COMPL IANT si AWS Shield Advanced está activado pero la función de acceso a SRT no está configura da.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-habilitado	Asegúrese de que un clúster de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	rds-instance-iam-authentication-habilitado	Asegúrese de que una instancia de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	shield-drt-access	Asegúrese de que el Shield Response Team (SRT) pueda acceder a su AWS cuenta. La regla es NON_COMPL IANT si AWS Shield Advanced está activado pero la función de acceso a SRT no está configura da.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-habilitado	Asegúrese de que un clúster de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.2	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	rds-instance-iam-authentication-habilitado	Asegúrese de que una instancia de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.
7.2.4	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específico de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	shield-drt-access	Asegúrese de que el Shield Response Team (SRT) pueda acceder a su AWS cuenta. La regla es NON_COMPLIANT si AWS Shield Advanced está activado pero la función de acceso a SRT no está configurada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-habilitado	Asegúrese de que un clúster de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.5	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	rds-instance-iam-authentication-habilitado	Asegúrese de que una instancia de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.
7.2.5.1	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específico de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.6	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.2.6	El acceso a los componentes y datos del sistema está definido y asignado adecuadamente. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	shield-drt-access	Asegúrese de que el Shield Response Team (SRT) pueda acceder a su AWS cuenta. La regla es NON_COMPLIANT si AWS Shield Advanced está activado pero la función de acceso a SRT no está configurada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-habilitado	Asegúrese de que un clúster de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.1	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	rds-instance-iam-authentication-habilitado	Asegúrese de que una instancia de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	shield-drt-access	Asegúrese de que el Shield Response Team (SRT) pueda acceder a su AWS cuenta. La regla es NON_COMPLIANT si AWS Shield Advanced está activado pero la función de acceso a SRT no está configurada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-habilitado	Asegúrese de que un clúster de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.2	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	rds-instance-iam-authentication-habilitado	Asegúrese de que una instancia de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	shield-drt-access	Asegúrese de que el Shield Response Team (SRT) pueda acceder a su AWS cuenta. La regla es NON_COMPLIANT si AWS Shield Advanced está activado pero la función de acceso a SRT no está configurada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-habilitado	Asegúrese de que un clúster de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
7.3.3	El acceso a los componentes y datos del sistema se administra a través de sistemas de control de acceso. (PCI-DSS-v4.0)	rds-instance-iam-authentication-habilitado	Asegúrese de que una instancia de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.
8.2.1	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.1	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-comprobar	Asegúrese de que el proyecto NO contenga variables de entorno ni AWS_ACCES S_KEY_ID AWS_SECRE T _ACCESS_K EY. La regla es NON_COMPLIANT si las variables de entorno del proyecto contienen credencia les de texto no cifrado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.2	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específico de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.
8.2.4	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.4	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.
8.2.5	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.5	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.
8.2.6	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	secretsmanager-sec ret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específic o de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	shield-drt-access	Asegúrese de que el Shield Response Team (SRT) pueda acceder a su AWS cuenta. La regla es NON_COMPL IANT si AWS Shield Advanced está activado pero la función de acceso a SRT no está configura da.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Managemen t (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autentica ción de base de datos de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-habilitado	Asegúrese de que un clúster de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.7	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	rds-instance-iam-authentication-habilitado	Asegúrese de que una instancia de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	shield-drt-access	Asegúrese de que el Shield Response Team (SRT) pueda acceder a su AWS cuenta. La regla es NON_COMPL IANT si AWS Shield Advanced está activado pero la función de acceso a SRT no está configura da.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administr adores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Managemen t (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autentica ción de base de datos de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-habilitado	Asegúrese de que un clúster de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec2-imdsv2-check	Asegúrese de que la versión de metadatos de su instancia de Amazon Elastic Compute Cloud (Amazon EC2) esté configurada con la versión 2 () de Instance Metadata Service. IMDSv2 La regla no cumple con los requisitos si HttpTokens se establece en opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	autoscaling-launchconfig-requires-imdsv2.	Asegúrese de que solo IMDSv2 esté activado. Esta regla es NON_COMPLIANT si la versión de metadatos no está incluida en la configuración de lanzamiento o si los metadatos V1 y V2 están habilitados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.2.8	La identificación de usuario y las cuentas relacionadas para los usuarios y administradores se administran estrictamente durante todo el ciclo de vida de la cuenta. (PCI-DSS-v4.0)	rds-instance-iam-authentication-habilitado	Asegúrese de que una instancia de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.
8.3.10.1	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccessKey La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.10.1	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.
8.3.10.1	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.11	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
8.3.11	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	ec-2 no-amazon-key-pair	Compruebe que las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución no se inicialicen con pares de claves de Amazon. La regla es NON_COMPLIANT si se lanza una instancia de EC2 en ejecución con un par de claves.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-descanso	Compruebe que haya un grupo de trabajo de Amazon Athena cifrado en reposo. La regla es NON_COMPLIANT si el cifrado de datos en reposo no está habilitado para un grupo de trabajo de Athena.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Compruebe que haya un clúster de base de datos de Amazon Neptune con instantáneas cifradas. La regla es NON_COMPLIANT si un clúster de Neptune no tiene las instantán eas cifradas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Asegúrese de que los clústeres de Amazon Redshift utilicen una AWS clave específica del Servicio de administración de claves (AWS KMS) para el cifrado. La regla cumple con las normas si el cifrado está activado y el clúster está cifrado con la clave proporcionada en el kmsKeyArn parámetro. La regla es NON_COMPLIANT si el clúster no está cifrado o está cifrado con otra clave.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	codebuild-project-artifact-encryption	Asegúrese de que un AWS CodeBuild proyecto tenga el cifrado activado para todos sus artefactos. La regla kms:DescribeKey si encryptionDisabled se establece en true para cualquier configura ción de artefacto principal o secundario (si está presente).
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	codebuild-project-sCifrado de 3 registros	Asegúrese de que un AWS CodeBuild proyecto configura do con Amazon S3 Logs tenga el cifrado activado para sus registros. La regla no cumple con los requisitos si «EncryptionDisable d» se establece en «verdadero» en el S3 de un proyecto. LogsConfig CodeBuild

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	dax-encryption-enabled	Compruebe que los clústeres del Acelerador de Amazon DynamoDB (DAX) estén cifrados. La regla es NON_COMPLIANT si el clúster de DAX no está cifrado.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) de los almacenes de datos de Redis estén habilitados para el TLS/SSL cifrado de los datos comunicados con otros puntos finales. La regla no cumple con los requisitos si el cifrado no está activado. TLS/SSL

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	eks-secrets-encrypted	Asegúrese de que los clústeres de Amazon Elastic Kubernetes Service estén configurados para cifrar AWS los secretos de Kubernetes mediante claves del Servicio de administración de claves (KMS).
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	api-gw-cache-enabled-y encriptado	Compruebe que todos los métodos de las etapas de Amazon API Gateway tengan memoria caché habilitada y cifrada. La regla es NON_COMPLIANT si algún método de una etapa de Amazon API Gateway no está configurada para el almacenamiento en caché o si la caché no está cifrada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	docdb-cluster-encrypted	Compruebe que el cifrado de almacenamiento esté habilitado en los clústeres de Amazon DocumentDB (compatible con MongoDB). La regla es NON_COMPLIANT si el cifrado de almacenamiento no está habilitado.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Asegúrese de que la tabla de Amazon DynamoDB esté cifrada AWS con el Servicio de administración de claves (KMS). La regla no es compatible si la tabla de Amazon DynamoDB no está cifrada con KMS. AWS La regla tampoco cumple con los requisitos si la clave de AWS KMS cifrada no está presente en el parámetro de entrada. kmsKeyArns

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	dynamodb-table-encryption-enabled	Compruebe que las tablas de Amazon DynamoDB estén cifradas y revise su estado. La regla es COMPLIANT si el estado indica que se han habilitado o se están habilitando.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocolos	Asegúrese de que CloudFront las distribuciones no utilicen protocolos SSL obsoletos para la comunicación HTTPS entre las ubicaciones de CloudFront borde y los orígenes personalizados. Esta regla no cumple con las condiciones de una CloudFront distribución si alguna OriginSslProtocols de ellas «incluye». SSLv3

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encriptado	Asegúrese de que CloudFron t las distribuc iones de Amazon estén cifrando el tráfico hacia orígenes personali zados. La regla NO CUMPLE CON LOS REQUISITO S si '' es 'solo http' o si '' es 'visor de coincidencias' y OriginProtocolPolicy '' es 'permitido todo'. OriginProtocolPolicy ViewerProtocolPolicy
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Asegúrese de que sus CloudFront distribuciones de Amazon utilicen HTTPS (directam ente o mediante una redirección). La regla no cumple con los requisitos si el valor de ViewerPro tocolPolicy está establecido en 'allow-all' para el o para el. DefaultCacheBehavi or CacheBehaviors

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-comprobar	Asegúrese de que el proyecto NO contenga variables de entorno ni _ACCESS_KEY. AWS_ACCESS_KEY_ID AWS_SECRET La regla es NON_COMPLIANT si las variables de entorno del proyecto contienen credenciales de texto no cifrado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Asegúrese de que su clúster de Amazon DynamoDB Accelerator (DAX) esté configurado en TLS. ClusterEndpointEncryptionType La regla es NON_COMPLIANT si hay un clúster de DAX que no está cifrado con seguridad de la capa de transporte (TLS).
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Asegúrese de que los clústeres de Amazon EKS no estén configurados para cifrar los secretos de Kubernetes mediante KMS. AWS La regla es NON_COMPLIANT si hay un clúster de EKS sin un recurso de encryptionConfig o si encryptionConfig no designa secretos como un recurso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Compruebe que los flujos de Amazon Kinesis estén cifrados en reposo con el cifrado en el servidor. La regla no es conforme para una transmisión de Kinesis si 'StreamEncryption' no está presente.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	msk-in-cluster-node-requerido-tls	Compruebe que haya un clúster de Amazon MSK que aplique el cifrado en tránsito con HTTPS (TLS) con los nodos de agente del clúster. La regla es NON_COMPLIANT si la comunicación de texto sin formato está habilitada para conexiones de nodo de agente dentro del clúster.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Compruebe que el cifrado de almacenamiento esté habilitado para los clústeres de base de datos de Amazon Neptune. La regla es NON_COMPLIANT si el cifrado de almacenamiento no está habilitado.
8.3.2	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Asegúrese de que los puntos finales del AWS Database Migration Service (AWS DMS) estén configurados con una conexión SSL. La regla NO ES COMPATIBLE si el AWS DMS no tiene configurada una conexión SSL.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	s3- bucket-blacklisted-actions-prohibited	Asegúrese de que la política de bucket de Amazon Simple Storage Service (Amazon S3) no permita acciones a nivel de bucket y a nivel de objeto incluidas en listas de bloqueos en los recursos del bucket para los directore s de otras cuentas. AWS Por ejemplo, la regla comprueba que la política de bucket de Amazon S3 no permite que otra AWS cuenta realice ninguna acción s3: GetBucket * ni s3: DeleteObject en ningún objeto del bucket. La regla es NON_COMPL IANT si la política de buckets de Amazon S3 permite alguna acción incluida en la lista de bloqueo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	s3- bucket-policy-not-more -permisivo	Compruebe que las políticas del bucket de Amazon Simple Storage Service (S3) no otorguen permisos entre cuentas distintos a los de la política del bucket de Amazon S3 de control que se haya proporcionado.
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	shield-drt-access	Asegúrese de que el Shield Response Team (SRT) pueda acceder a su AWS cuenta. La regla es NON_COMPLIANT si AWS Shield Advanced está activado pero la función de acceso a SRT no está configurada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	iam-policy-in-use	Compruebe que el ARN de la política de IAM esté asociado a un usuario de IAM, o a un grupo con uno o varios usuarios de IAM, o a un rol de IAM con una o varias entidades de confianza.
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	neptune-cluster-iam-database-autenticación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la autenticación de bases de datos AWS Identity and Access Management (IAM). La regla es NON_COMPLIANT si un clúster de Amazon Neptune no tiene habilitada la autenticación de base de datos de IAM.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-habilitado	Asegúrese de que un clúster de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) (Identity and Access Management). La regla es NON_COMPLIANT si un clúster de Amazon RDS no tiene habilitada la autenticación de IAM.
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	ec-2 instance-profile-attached	Asegúrese de que una instancia EC2 tenga un AWS perfil de Identity and Access Management (IAM) adjunto. La regla es NON_COMPLIANT si no hay ningún perfil de IAM asociado a la instancia de EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.4	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	rds-instance-iam-authentication-habilitado	Asegúrese de que una instancia de Amazon Relational Database Service (Amazon RDS) AWS tenga habilitada la autenticación Identity and Access Management (IAM) Access Management (IAM). La regla es NON_COMPLIANT si una instancia de Amazon RDS no tiene habilitada la autenticación de IAM.
8.3.5	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccessKey La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.5	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.
8.3.5	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.7	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccess Key La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.
8.3.7	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.7	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.
8.3.9	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccessKey La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.3.9	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.
8.3.9	Se ha establecido y administrado una autenticación sólida para los usuarios y los administradores. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.4.1	Se ha implement ado la autenticación multifactor (MFA) para proteger el acceso al CDE. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitad a en la configura ción del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.
8.4.2	Se ha implement ado la autenticación multifactor (MFA) para proteger el acceso al CDE. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitad a en la configura ción del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.4.3	Se ha implement ado la autenticación multifactor (MFA) para proteger el acceso al CDE. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitad a en la configura ción del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.
8.6.3	El uso de las cuentas de aplicación y sistema, y de los factores de autentica ción asociados, se gestiona de forma rigurosa. (PCI-DSS-v4.0)	access-keys-rotated	Asegúrese de que las claves de acceso de IAM activas se roten (cambien) dentro del número de días especificado en Age. maxAccess Key La regla es NON_COMPLIANT si las claves de acceso no se rotan dentro del período de tiempo especificado. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.6.3	El uso de las cuentas de aplicación y sistema, y de los factores de autenticación asociados, se gestiona de forma rigurosa. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-comprobar	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado correctamente de acuerdo con el programa de rotación. Secrets Manager calcula la fecha en que debe producirse la rotación. La regla es NON_COMPLIANT si pasa la fecha y el secreto no rota.
8.6.3	El uso de las cuentas de aplicación y sistema, y de los factores de autenticación asociados, se gestiona de forma rigurosa. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Asegúrese de que AWS los secretos de Secrets Manager se hayan rotado en los últimos días especificados. La regla no cumple con los requisitos si un secreto no se ha rotado durante más de un número de días de maxDaysSince rotación. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibido	Compruebe que haya una instantánea manual de un clúster de base de datos de Amazon Neptune que no sea pública. La regla es NON_COMPLIANT si las instantáneas de clústeres nuevas y existentes de Neptune son públicas.
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibido	Compruebe que las instantáneas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	backup-recovery-point-manual-eliminación-deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no cumple con los requisitos si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.
A1.1.2	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	api-gw-endpoint-type-comprobar	Asegúrese de que Amazon API Gateway APIs sea del tipo especificado en el parámetro de regla 'endpoint ConfigurationType' . La regla devuelve NON_COMPLIANT si la API REST no coincide con el tipo de punto de enlace configurado en el parámetro de regla.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Asegúrese de que CloudFront las distribuciones de Amazon estén asociadas al firewall de aplicaciones web (WAF) o a las listas de control de acceso WAFv2 web (ACLs). La regla no cumple con los requisitos si una CloudFront distribución no está asociada a una ACL web de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Asegúrese de que el certificado asociado a una CloudFron t distribución de Amazon no sea el certificado SSL predeterminado. La regla no es conforme si una CloudFront distribución utiliza el certificado SSL predeterminado.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	netfw-policy-default-action-paquetes de fragmentos	Asegúrese de que la política AWS de Network Firewall esté configurada con una acción predeterminada sin estado definida por el usuario para los paquetes fragmenta dos. La regla es NON_COMPLIANT si la acción predeterm inada sin estado para los paquetes fragmentados no coincide con la acción predeterm inada definida por el usuario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	rds-db-security-group-no permitido	Compruebe que los grupos de seguridad de base de datos de Amazon Relationa l Database Service (Amazon RDS) sean los predeterm inados. La regla es NON_COMPLIANT si hay algún grupo de seguridad de base de datos que no sea el grupo de seguridad de base de datos predeterminado.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	ec2- -attach-d esactivado transit-g ateway-auto-vpc	Asegúrese de que las pasarelas de tránsito de Amazon Elastic Compute Cloud (Amazon EC2) no tengan " activado. AutoAcceptSharedAt tachments La regla no es conforme para una Transit Gateway si 'AutoAcceptSharedA ttachments' está configurada como 'activa'.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	eks-endpoint-no-public-acceso	Compruebe que el punto de conexión de Amazon Elastic Kubernetes Service (Amazon EKS) no sea de acceso público. La regla es NON_COMPLIANT si el punto de conexión es de acceso público.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	restricted-ssh	Nota: Para esta regla, el identificador de la regla (INCOMING_SSH_DISABLED) y el nombre de la regla (restricted-ssh) son diferentes. Compruebe que el tráfico SSH entrante de los grupos de seguridad sea accesible. La regla es COMPLIANT si las direcciones IP del tráfico SSH entrante en los grupos de seguridad están restringidas (un CIDR distinto de 0.0.0.0/0 o ::/0). De lo contrario, es NON_COMPLIANT.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	appsync-associated-with-waf	Asegúrese de que AWS AppSync APIs estén asociadas a las listas de control de acceso AWS WAFv2 web (). ACLs La regla no es compatibl e con una AWS AppSync API si no está asociada a una ACL web.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	docdb-cluster-snap shot-public-prohibido	Compruebe que las instantán eas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	codebuild-project-source-repo-comprobación de URL	Compruebe que la URL del repositorio fuente de Bitbucket NO contenga credenciales de inicio de sesión. La regla es NON_COMPLIANT si la URL contiene información de inicio de sesión y COMPLIANT si no la contiene.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	elb-acm-certificate-required	Asegúrese de que los balanceadores de carga clásicos usen certificados SSL proporcionados por AWS Certificate Manager. Para usar esta regla, utilice un agente de escucha SSL o HTTPS con su Classic Load Balancer. Nota: Esta regla solo se aplica a los equilibradores de carga clásicos. Esta regla no comprueba los Application Load Balancers ni los Network Load Balancers.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no es compatible si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Asegúrese de que los puertos predeterminados para el tráfico SSH/RDP de entrada de las listas de control de acceso a la red (NACLs) estén restringidos. La regla es NON_COMPLIANT si una entrada entrante de la NACL permite un bloque CIDR TCP o UDP de origen para los puertos 22 o 3389.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	waf-global-webacl-not-vacío	Compruebe que haya una ACL web de WAF Global que contenga reglas o grupos de reglas de WAF. Esta regla es NON_COMPLIANT si una ACL web no contiene reglas ni grupos de reglas de WAF.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	waf-global-rulegroup-not-vacío	Asegúrese de que un grupo de reglas AWS de WAF Classic contenga algunas reglas. La regla es NON_COMPLIANT si no hay reglas en un grupo de reglas.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	waf-global-rule-not-vacío	Asegúrese de que una regla global AWS de WAF contenga algunas condicion es. La regla es NON_COMPLIANT si no hay condiciones presentes en la regla global de WAF.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	ec2- -todos client-vpn-not-authorize	Asegúrese de que las reglas de autorización de AWS Client VPN no autoricen el acceso a la conexión para todos los clientes. La regla es NON_COMPLIANT si 'AccessAll' está presente y se establece en true.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-solo	Compruebe que las puertas de enlace de Internet estén asociadas a una nube privada virtual autorizada (Amazon VPC). La regla es NON_COMPLIANT si las puertas de enlace de Internet están conectadas a una VPC no autorizada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
A1.1.3	Los proveedores de servicio multinquilino protegen y separan todos los entornos y datos de los clientes. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	api-gwv2- access-lo gs-enabled	Compruebe que las etapas de Amazon API Gateway V2 tengan habilitad o el registro de acceso. La regla no es compatible si 'accessLogSettings' no está presente en la configuración del escenario.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	cloudfront-accessl ogs-enabled	Asegúrese de que CloudFront las distribuciones de Amazon estén configuradas para entregar los registros de acceso a un bucket de Amazon S3. La regla no cumple con los requisitos si una CloudFront distribuc ión no tiene el registro configurado.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Asegúrese de que haya al menos un AWS CloudTrail registro definido con las mejores prácticas de seguridad. Esta regla es COMPLIANT si hay al menos un registro de seguimien to que cumpla todos los requisitos siguientes:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	neptune-cluster-cl oudwatch-log-habil itado para exportación	Asegúrese de que un clúster de Amazon Neptune tenga habilitada la exportaci ón de CloudWatc h registros para los registros de auditoría . La regla no es compatible si un clúster de Neptune no tiene habilitad a la exportación de registros para los CloudWatch registros de auditoría.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	ecs-task-definition-log-configuración	Compruebe que logConfiguration esté configurado como activo en las definiciones de tareas de Amazon ECS. Esta regla NO ES COMPATIBLE si una ECSTask definició n activa no tiene definido el recurso LogConfiguration o si el valor de LogConfig uration es nulo en al menos una definición de contenedor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	cloudtrail-enabled	Nota: Para esta regla, el identificador de la regla (CLOUD_TR AIL_ENABLED) y el nombre de la regla (cloudtrail-enable d) son diferente s. Asegúrese de que haya una AWS CloudTrail ruta habilitada en su cuenta. AWS La regla es NON_COMPL IANT si no hay ningún registro de seguimien to habilitado. De forma opcional, la regla comprueba un bucket de S3, un tema de Amazon Simple Notification Service (Amazon SNS) y un grupo de registros específicos. CloudWatch

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Nota: para esta regla, el identificador de la regla (MULTI_RE GION_CLOU D_TRAIL_ENABLED) y el nombre de la regla () son diferente s. multi-region-cloudtrail-enabled Asegúrese de que haya al menos una región múltiple. AWS CloudTrail La regla es NON_COMPL IANT si los registros de seguimiento no coinciden con los parámetros de entrada. La regla es NON_COMPL IANT si el ExcludeMa nagementEventSourc es campo no está vacío o si AWS CloudTrail está configurado para excluir eventos de administración, como eventos de AWS KMS o eventos de Amazon RDS Data API.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	appsync-logging-en abled	Asegúrese de que la AWS AppSync API tenga habilitado el registro. La regla NO ES COMPATIBLE si el registro no está habilitado o «fieldLog Level» no es ERROR ni ALL.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Asegúrese de que el registro esté habilitad o en las listas de control AWS de acceso web globales (web) clásicas de WAF. ACLs La regla es NON_COMPLIANT para una ACL web global si no tiene el registro activado.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-habilitado	Asegúrese de que los agentes de Amazon MQ tengan activado el registro de CloudWatch auditoría de Amazon. La regla es NON_COMPLIANT si un agente no tiene activado el registro de auditoría.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-habilitado	Asegúrese de que un agente de Amazon MQ tenga activado el registro CloudWatch de auditoría. La regla es NON_COMPLIANT si el agente no tiene habilitado el registro de auditoría.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Compruebe que haya un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) configurado y con el registro habilitado. La regla es NON_COMPLIANT si el registro de los clústeres de Amazon EKS no está habilitad o para todos los tipos de registro.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to- vigilancia en la nube	Asegúrese de que los entornos de AWS Elastic Beanstalk estén configurados para enviar registros a Amazon Logs. CloudWatch La regla no es conforme si el valor de `` es falso. StreamLogs

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	step-functions-state-machine-habilitado para el registro	Asegúrese de que la máquina AWS Step Functions tenga activado el registro. La regla es NON_COMPLIANT si una máquina de estado no tiene el registro activado o si la configuración de registro no se encuentra en el nivel mínimo indicado.
A1.2.1	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	netfw-logging-enabled	Asegúrese de que los firewalls de AWS Network Firewall tengan habilitado el registro. La regla es NON_COMPLIANT si el tipo de registro no está configurado. Puede especificar qué tipo de registro desea que compruebe la regla.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A1.2.3	Los proveedores de servicios multinqui lino facilitan el registro y la respuesta a los incidentes para todos los clientes. (PCI-DSS-v4.0)	security-account-information-provided	Asegúrese de haber proporcionado la información de contacto de seguridad de los contactos de su AWS cuenta. La regla es NON_COMPLIANT si no se proporcio na la información de contacto de seguridad de la cuenta.
A3.2.5.1	El ámbito del PCI DSS está documenta do y validado. (PCI-DSS-v4.0)	macie-auto-sensitive-data-comprobación-descubrimiento	Compruebe que la detección automatiz ada de datos confidenciales esté habilitada en Amazon Macie. La regla es NON_COMPL IANT si la detección automatizada de datos confidenciales está deshabilitada. La regla es APPLICABL E para las cuentas de administrador y NOT_APPLICABLE para las cuentas de los miembros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.2.5.1	El ámbito del PCI DSS está documentado y validado. (PCI-DSS-v4.0)	macie-status-check	Compruebe que Amazon Macie esté activado en su cuenta por región. La regla es NON_COMPLIANT si el atributo Status no se ha definido como ENABLED.
A3.2.5.2	El ámbito del PCI DSS está documentado y validado. (PCI-DSS-v4.0)	macie-auto-sensitive-data-comprobación-descubrimiento	Compruebe que la detección automatizada de datos confidenciales esté habilitada en Amazon Macie. La regla es NON_COMPLIANT si la detección automatizada de datos confidenciales está deshabilitada. La regla es APPLICABLE para las cuentas de administrador y NOT_APPLICABLE para las cuentas de los miembros.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.2.5.2	El ámbito del PCI DSS está documenta do y validado. (PCI-DSS-v4.0)	macie-status-check	Compruebe que Amazon Macie esté activado en su cuenta por región. La regla es NON_COMPLIANT si el atributo Status no se ha definido como ENABLED.
A3.3.1	El PCI DSS está incorporado a las actividades de business-as-usual (BAU). (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades business-as-usual (BAU). (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Asegúrate de que tus CloudFormation stacks envíen notificaciones de eventos a un tema de Amazon SNS. Como característica opcional, compruebe que se estén utilizando los temas de Amazon SNS especificados. La regla no cumple con los requisitos si las CloudFormation pilas no envían notificaciones.
A3.3.1	El PCI DSS está incorporado business-as-usual a las actividades (BAU). (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitado la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de la (BAU). business-as-usual (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
A3.3.1	El PCI DSS está incorporado a las actividades business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan los ajustes especificados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.3.1	El PCI DSS está incorporado a las actividades de business-as-usual (BAU). (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.
A3.3.1	El PCI DSS está incorporado a las actividades de business-as-usual (BAU). (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibido	Compruebe que haya una instantánea manual de un clúster de base de datos de Amazon Neptune que no sea pública. La regla es NON_COMPLIANT si las instantáneas de clústeres nuevas y existentes de Neptune son públicas.
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibido	Compruebe que las instantáneas de clúster manual de Amazon DocumentDB no sean públicas. La regla es NON_COMPLIANT si alguna instantánea de clúster manual de Amazon DocumentDB es pública.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	backup-recovery-point-manual- eliminación: deshabilitada	Compruebe que haya un almacén de copia de seguridad con una política basada en recursos asociada que impida la eliminación de los puntos de recuperación. La regla no es compatible si Backup Vault no tiene políticas basadas en recursos o tiene políticas sin una declaración de «Denegar» adecuada (declaración con permisos de backup:DeleteRecoveryPoint, backup: y backup:UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	emr-block-public-access	Compruebe que haya una cuenta de Amazon EMR con la configuración de bloqueo de acceso público habilitada. La regla no cumple con los requisitos si BlockPublicSecurityGroupRules es falsa o, si es verdadera, aparecen los puertos distintos del puerto 22. Permitted PublicSecurityGroupRuleRanges
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Asegúrese de que se AWS haya accedido a los secretos de Secrets Manager en un número específico de días. La regla no cumple con los requisitos si no se ha accedido a un secreto en un número «unusedForDays» de días. El valor predeterminado es 90 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	bloques s3 access-point-public-access -	Compruebe que los puntos de acceso de Amazon S3 tengan habilitada la configuración de bloqueo del acceso público. La regla NON_COMPLIANT si la configuración de bloqueo de acceso público no está habilitada para los puntos de acceso de S3.
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	bloques s3 account-level-public-access -	Compruebe que la configuración requerida del bloqueo de acceso público se haya configurado desde el nivel de cuenta. La regla sólo es NON_COMPLIANT cuando los campos establecidos a continuación no coinciden con los campos correspondientes en el elemento de configuración.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.4.1	El acceso lógico al entorno de datos del titular de la tarjeta está controlado y administrado. (PCI-DSS-v4.0)	s3- bucket-mfa-delete-enabled	Compruebe que la eliminación de la MFA esté habilitada en la configuración del control de versiones de buckets de Amazon Simple Storage Service (Amazon S3). La regla es NON_COMPLIANT si la eliminación de MFA no está habilitada.
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	api-gw-xray-enabled	Asegúrese de que el rastreo de AWS X-Ray esté habilitado en Amazon API Gateway APIs REST. La regla es COMPLIANT si el rastreo de X-Ray está habilitado y NON_COMPLIANT cuando no lo está.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Asegúrate de que tus CloudForm ation stacks envíen notificaciones de eventos a un tema de Amazon SNS. Como caracterí stica opcional, compruebe que se estén utilizando los temas de Amazon SNS especificados. La regla no cumple con los requisitos si las CloudForm ation pilas no envían notificaciones.
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	ec-2 instance-detailed-monitoring-enabled	Compruebe que se haya habilitad o la monitorización detallada para las instancias de EC2. La regla es NON_COMPLIANT si la supervisión detallada no está habilitada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Asegúrese de que CloudWatch las alarmas tengan una acción configurada para los estados ALARM, INSUFFICIENT_DATA o OK. Como factor opcional, compruebe que haya acciones que coincidan con un ARN indicado. La regla es NON_COMPLIANT si no se ha especificado ninguna acción para la alarma o el parámetro opcional.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Asegúrese de que un tipo de recurso tenga una CloudWatch alarma para la métrica indicada. Para el tipo de recurso, puede especificar volúmenes de EBS, instancias de EC2, clústeres de Amazon RDS o buckets de S3. La regla cumple con las normas si la métrica indicada tiene un identificador de recurso y una CloudWatch alarma.
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Asegúrese de que CloudWatch las alarmas con el nombre de métrica indicado tengan la configuración especificada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	guerra 2- rulegroup-logging-enabled	Asegúrese de que la recopilación CloudWatch de métricas de seguridad de Amazon en los grupos de AWS WAFv2 reglas esté habilitada. La regla no cumple con los requisitos si el signo '. VisibilityConfig CloudWatchMetricsEnabledel campo 'está establecido en falso.
A3.5.1	Los eventos sospechosos se identifican y se responde a ellos. (PCI-DSS-v4.0)	sns-topic-message-delivery-habilitado para notificaciones	Compruebe que el registro de Amazon Simple Notification Service (SNS) esté habilitado para el estado de entrega de los mensajes de notificación enviados a un tema para los puntos de conexión. La regla es NON_COMPLIANT si la notificación del estado de entrega de los mensajes no está habilitada.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para PCI DSS 4.0 (incluidos los tipos de recursos globales).

Prácticas operativas recomendadas para recursos de acceso público

Este paquete de conformidad ayuda a identificar los recursos que pueden ser de acceso público.

Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para recursos de acceso público.

Mejores prácticas operativas para el marco de ciberseguridad del RBI para UCBs

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas AWS Config y acciones correctivas. AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación se proporciona un ejemplo de mapeo entre el Marco de Ciberseguridad del Banco de la Reserva de la India (RBI) para los bancos cooperativos urbanos (UCBs) y las reglas de Config AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más marcos de ciberseguridad del RBI para UCBs los controles. Un marco de ciberseguridad de RBI para el UCBs control puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.1)	ec2- -manager instance-managed-by-systems	Es posible realizar un inventari o de las plataformas y aplicaciones de software de

ID de control	AWS Regla de configuración	Directrices
		la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
Anexo_I (1.1)	account-part-of-organizations	La administración centralizada Cuentas de AWS dentro de AWS Organizations ayuda a garantizar que las cuentas cumplan con las normas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.1)	ecr-private-tag-immutability-habilitado	Se activa la inmutabilidad de las etiquetas del Elastic Container Repository (ECR) para evitar que se sobrescri ban las etiquetas de las imágenes de ECR. Anteriorm ente, las etiquetas podían sobrescribirse, lo que requería metodologías manuales para identificar de forma exclusiva una imagen.
Anexo_I (1.3)	acm-certificate-expiration-check	Asegúrese de que la integrida d de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundament ales: 90). El valor real debe reflejar las políticas de su organización.
Anexo_I (1.3)	alb-http-drop-invalid-encab ezado activado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenc iales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicación redirija automáticamente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo_I (1.3)	api-gw-cache-enabled-y encriptado	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté activado en la caché de la etapa de API Gateway. Puesto que pueden capturarse datos confidenc iales para el método de la API, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo_I (1.3)	cloud-trail-encryption-enabled	Como es posible que existan datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté activado en tus registros AWS CloudTrail .

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certifica dos SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.
Anexo_I (1.3)	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certifica dos públicos y privados con AWS servicios y recursos internos.
Anexo_I (1.3)	s3- default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos confidenciales en reposo, asegúrate de que el cifrado esté activado en tus Amazon CloudWatch Log Groups.
Anexo_I (1.3)	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
Anexo_I (1.3)	backup-recovery-point-encrypted	Asegúrese de que el cifrado esté activado en sus puntos AWS de recuperación de Backup. Puesto que puede haber datos confidenciales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo_I (1.3)	codebuild-project-artifact-encryption	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado de sus AWS CodeBuild artefactos esté activado.
Anexo_I (1.3)	codebuild-project-s3 registros cifrados	Para ayudar a proteger los datos confidenciales en reposo, asegúrese de que el cifrado esté habilitado para AWS CodeBuild los registros almacenados en Amazon S3.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	opensearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch Service.
Anexo_I (1.3)	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
Anexo_I (1.3)	opensearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	dynamodb-table-encrypted-kms	Asegúrese de que el cifrado esté habilitado para las tablas de Amazon DynamoDB. Puesto que puede haber datos confidenciales en reposo en estas tablas, habilite el cifrado en reposo para ayudar a protegerlos. De forma predeterminada, las tablas de DynamoDB se AWS cifran con una clave maestra del cliente (CMK) propia.
Anexo_I (1.3)	ec2- ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenciales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo_I (1.3)	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	elasticsearch-encrypted-at-rest	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en reposo, asegúrate de que el cifrado esté habilitado para tus dominios de Amazon OpenSearch OpenSearch Service (Servicio).
Anexo_I (1.3)	elasticsearch-node-to-node-verificación de cifrado	Asegúrese de que el node-to-node cifrado OpenSearch de Amazon Service esté activado. Node-to-nodeel cifrado permite el cifrado TLS 1.2 para todas las comunicaciones dentro de Amazon Virtual Private Cloud (Amazon VPC). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo_I (1.3)	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo_I (1.3)	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
Anexo_I (1.3)	kms-cmk-not-scheduled-para su eliminación	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMKs) necesarias no estén programadas para su eliminación en el Servicio de administración de AWS claves (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	rds-snapshot-encrypted	Asegúrese de que el cifrado esté habilitado para las instantáneas de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenc iales en reposo, habilite el cifrado en reposo para ayudar a protegerlos.
Anexo_I (1.3)	rds-storage-encrypted	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado esté habilitad o para sus instancias de Amazon Relational Database Service (Amazon RDS). Puesto que puede haber datos confidenciales en reposo en las instancias de Amazon RDS, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
Anexo_I (1.3)	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	habilitado para s3 bucket-server-side-encryption	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
Anexo_I (1.3)	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
Anexo_I (1.3)	sagemaker-endpoint-configuration-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su terminal. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker punto final, habilite el cifrado en reposo para ayudar a proteger esos datos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	sagemaker-notebook-instance-kms-configurado por clave	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado en su portátil. SageMaker Como los datos confidenciales pueden estar en reposo en el SageMaker portátil, habilite el cifrado en reposo para ayudar a proteger esos datos.
Anexo_I (1.3)	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas del Amazon Simple Notification Service (Amazon SNS) requieran cifrado AWS mediante el Servicio AWS de administr ación de claves (KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancia s de replicación del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Anexo_I (1.3)	ebs-snapshot-public-restora ble-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicamente. Las instantán eas de volumen de EBS pueden contener información confidencial y dichas cuentas requieren control de acceso.
Anexo_I (1.3)	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.
Anexo_I (1.3)	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	ec2- instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	autoscaling-launch-config-public-IP deshabilitada	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
Anexo_I (1.3)	no-unrestricted-route-to-igw	Asegúrese de que las tablas de enrutamiento de Amazon EC2 no tengan rutas ilimitadas a una puerta de enlace de internet. Eliminar o limitar el acceso a Internet para las cargas de trabajo en Amazon VPCs puede reducir el acceso no deseado dentro de su entorno.
Anexo_I (1.3)	redshift-cluster-kms-enabled	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con el Servicio de administración de AWS claves (AWS KMS) esté habilitado para su clúster de Amazon Redshift. Puesto que puede haber datos confidenciales en reposo en los clústeres de Redshift, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.
Anexo_I (1.3)	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automátic amente una dirección IP pública. Las instancias de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	internet-gateway-authorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.
Anexo_I (1.3)	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicación segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositi vo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.
Anexo_I (1.3)	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relational Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidencial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principio s. Además dichas cuentas requieren control de acceso.
Anexo_I (1.3)	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configura r opcionalmente los restrictP ublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.
Anexo_I (1.3)	s3- bucket-public-read-prohibit ed	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositi vos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (1.3)	s3- bucket-public-write-prohibited	Gestione el acceso a los recursos de la AWS nube permitiendo que solo los usuarios, procesos y dispositivos autorizados accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
Anexo_I (1.3)	sagemaker-notebook-no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (5.1)	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicacio nes web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabi lidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.
Anexo_I (5.1)	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringi r todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos. AWS
Anexo_I (5.1)	waf-regional-rule-not-vacío	Asegúrese de que su AWS WAF tenga una regla que no esté vacía. Una regla sin condiciones podría desencade nar un comportamiento no deseado.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (5.1)	waf-regional-rulegroup-not-vacío	Asegúrese de que su AWS WAF tenga un grupo de reglas que no esté vacío. Un grupo de reglas vacío podría desencadenar un comportamiento no deseado.
Anexo_I (5.1)	waf-regional-webacl-not-vacío	Una ACL web adjunta a un AWS WAF puede contener un conjunto de reglas y grupos de reglas para inspeccionar y controlar las solicitudes web. Si una ACL web está vacía, el tráfico web pasa sin que el WAF lo detecte ni actúe sobre él.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (5.1)	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (5.1)	api-gw-associated-with-guerra	AWS El WAF le permite configurar un conjunto de reglas (denominadas listas de control de acceso web (ACL web)) que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su etapa de Amazon API Gateway esté asociada a una ACL web de WAF para protegerla de ataques maliciosos.
Anexo_I (5.1)	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (5.1)	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (6)	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataform as y aplicaciones de software dentro de una organizac ión. AWS Systems Manager asigna un estado de configura ción a las instancias administr adas y le permite establecer líneas base de los niveles de parches del sistema operativo , las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.
Anexo_I (6)	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documenta r las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (6)	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.
Anexo_I (6)	elastic-beanstalk-managed-updates-activado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (6)	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancia s de Amazon Relational Database Service (RDS) para garantizar que estén instalada s las últimas actualizaciones de las versiones secundari as del sistema de administr ación de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (6)	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el. allowVersionUpgrade El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.
Anexo_I (6)	vuln-management-plan-exists (verificación del proceso)	Garantizar que se desarrolle e implemente un plan de administración de vulnerabilidades para disponer de procesos bien definidos para abordar las vulnerabilidades de su entorno.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.1)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
Anexo_I (7.1)	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.1)	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.
Anexo_I (7.1)	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegios.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.1)	iam-no-inline-policy-comprobar	Asegúrese de que un usuario, rol de IAM o grupo de IAM (AWS Identity and Access Management) no tenga una política integrada para controlar el acceso a los sistemas y activos. AWS recomienda utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.2)	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos establecidos por la norma NIST SP 800-63 y el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñas. Esta regla le permite configura r opcionalmente RequireUp percaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLo wercaseCharacters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundamentales: verdadero), RequireNumbers (valor de las mejores prácticas de seguridad AWS AWS fundamentales: verdadero), MinimumPasswordLen gth (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePrevention

ID de control	AWS Regla de configuración	Directrices
		(valor de las mejores prácticas de seguridad AWS fundament ales: 24) y MaxPasswordAge (valor de las mejores prácticas de seguridad fundamentales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.
Anexo_I (7.3)	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado estatal del tráfico de red de entrada y salida a los recursos. AWS AI no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
Anexo_I (7.4)	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.4)	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
Anexo_I (7.4)	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identificar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.
Anexo_I (7.4)	cloudtrail-s3-dataevents-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.4)	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.
Anexo_I (7.4)	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos , de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.4)	cw-loggroup-retention-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros, a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibl es dificulta la reconstrucción e identificación de eventos potencialmente maliciosos.
Anexo_I (7.4)	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilad os proporcionan información detallada sobre las solicitud es enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.4)	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilación se envíen a Amazon CloudWatch o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilación proporcionan información detallada sobre el proyecto de compilación.
Anexo_I (7.4)	opensearch-audit-logging-enabled	Asegúrese de que el registro de auditoría esté habilitado en sus dominios OpenSearch de Amazon Service. El registro de auditoría le permite realizar un seguimiento de la actividad de los usuarios en sus OpenSearch dominios, incluidas las autenticaciones correctas y fallidas, las solicitudes OpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.4)	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta . OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
Anexo_I (7.4)	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.4)	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaro n las llamadas y cuándo se produjeron. CloudTrai l entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.4)	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexi ones, consultas o tablas consultadas.
Anexo_I (7.4)	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.4)	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
Anexo_I (7.4)	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (7.4)	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar informaci ón acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezc a un valor para clusterDb Encrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organizac ión.
Anexo_I (10.2)	security-awareness-program-exists (verificación de proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (12)	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automátic amente una instantánea de volumen de almacenam iento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.
Anexo_I (12)	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (12)	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.
Anexo_I (12)	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas . Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (12)	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (12)	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (12)	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (12)	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organizac ión. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.
Anexo_I (12)	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatiz adas. Cuando las instantán eas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantán ea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (12)	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
Anexo_I (12)	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	AWS Regla de configuración	Directrices
Anexo_I (12)	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el marco de ciberseguridad del RBI para UCBs.

Prácticas operativas recomendadas para RBI MD-ITF

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante reglas gestionadas o personalizadas y acciones correctivas. AWS Config AWS Config Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de mapeo entre la Dirección Maestra del Banco de la Reserva de la India (RBI): el Marco de Tecnología de la Información y las reglas de Config AWS gestionadas. Cada regla de Config se aplica a un AWS recurso específico y se refiere a uno o más controles de RBI Master Direction — Information Technology Framework. Un control del RBI MD-ITF

puede estar relacionado con varias reglas de Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(a)	Identificación y clasificación de los activos de informaci ón.	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administr ación de las instancia s de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios , instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.
3.1(a)	Identificación y clasificación de los	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de

ID de control	Descripción del control	AWS Regla de configuración	Directrices
	activos de informaci ón.		referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancias de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.
3.1(a)	Identificación y clasificación de los activos de informaci ón.	ec2- volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancia s de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminación al finalizar una instancia. Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcional idad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(a)	Identificación y clasificación de los activos de información.	ecr-private-tag-immutability-habilitado	Se activa la inmutabilidad de las etiquetas del Elastic Container Repository (ECR) para evitar que se sobrescriban las etiquetas de las imágenes de ECR. Anteriormente, las etiquetas podían sobrescribirse, lo que requería metodologías manuales para identificar de forma exclusiva una imagen.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administrar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principales existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribución de claves (KDC). Este proporciona un medio para que las entidades principales se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada uno de las entidades principales.
3.1(c)	Control de acceso basado en roles	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	efs-access-point-enforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	efs-access-point-enforce-identidad de usuario	Para ayudar a implementar el principio de privilegios mínimos, asegúrese de que la aplicación por parte de los usuarios esté habilitada en su Amazon Elastic File System (Amazon EFS). Cuando está habilitado, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	iam-group-has-users-compruebe	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	ec2- instance-profile-attached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
3.1(c)	Control de acceso basado en roles	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(c)	Control de acceso basado en roles	secretsmanager-rotation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.
3.1(c)	Control de acceso basado en roles	secretsmanager-scheduled-rotation-success-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribuido correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(g)	Administración de incidentes	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(g)	Administración de incidentes	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(g)	Administración de incidentes	alb-waf-enabled	Asegúrese de que el AWS WAF esté habilitado en Elastic Load Balancers (ELB) para ayudar a proteger las aplicaciones web. Un WAF ayuda a proteger sus aplicaciones web o APIs contra los ataques web más comunes. Estas vulnerabilidades de la web pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos en su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(g)	Administración de incidentes	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(g)	Administración de incidentes	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
3.1(h)	Registros de seguimiento	api-gw-execution-logging-habilitado	El registro de API Gateway muestra vistas detalladas de los usuarios que han accedido a la API y la forma en que han accedido a la API. Esta información permite ver las actividades de los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	cloud-trail-cloud-watch-habilitado para registros	Usa Amazon CloudWatch para recopilar y gestionar de forma centralizada la actividad de los eventos de registro. La inclusión de AWS CloudTrail datos proporciona detalles de la actividad de llamadas a la API en su interior Cuenta de AWS.
3.1(h)	Registros de seguimiento	codebuild-project-logging-enabled	Asegúrese de que el registro de AWS CodeBuild proyectos esté habilitado para que los registros de salida de la compilaci ón se envíen a Amazon CloudWatc h o a Amazon Simple Storage Service (Amazon S3). Los registros de salida de la compilaci ón proporcionan información detallada sobre el proyecto de compilación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	opensearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. OpenSearch Los registros de errores del servicio pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.
3.1(h)	Registros de seguimiento	redshift-audit-logging-enabled	Para recopilar información sobre las conexiones y las actividades de los usuarios en su clúster de Amazon Redshift, asegúrese de que el registro de auditoría esté habilitado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	cloudtrail-enabled	AWS CloudTrail pueden ayudar a evitar el repudio al registrar las acciones de la consola AWS de administración y las llamadas a la API. Puede identific ar a los usuarios y a quién llamó a un AWS servicio, la dirección IP de origen en la Cuentas de AWS que se generaron las llamadas y los horarios de las llamadas. Los detalles de los datos capturados se muestran en el contenido del AWS CloudTrail registro.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	cloudtrail-s3-data events-enabled	La recopilación de eventos de datos del Simple Storage Service (Amazon S3) ayuda a detectar cualquier actividad anómala. Los detalles incluyen Cuenta de AWS información sobre el acceso a un bucket de Amazon S3, la dirección IP y la hora del evento.
3.1(h)	Registros de seguimiento	cw-loggroup-retent ion-period-comprobar	Asegúrese de que los datos del registro de eventos se conserven durante un tiempo mínimo para sus grupos de registros , a fin de facilitar la resolución de problemas y las investigaciones forenses. La falta de datos de registros de eventos anteriores disponibles dificulta la reconstrucción e identificación de eventos potencial mente maliciosos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	elasticsearch-logs-to-cloudwatch	Asegúrese de que los dominios de Amazon OpenSearch Service tengan los registros de errores habilitados y transmitidos a Amazon CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar en las auditorías de seguridad y acceso, además de para diagnosticar problemas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	elb-logging-enabled	La actividad de Elastic Load Balancing es un punto central de comunicación dentro de un entorno. Asegúrese de que el registro de ELB esté habilitado. Los datos recopilados proporcio nan información detallada sobre las solicitudes enviadas al ELB. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud , la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	multi-region-cloudtrail-enabled	AWS CloudTrail registra las acciones AWS de la consola de administración y las llamadas a la API. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. CloudTrail entregará los archivos de registro de todas AWS las regiones a su bucket de S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED está activado. Además, al AWS lanzar una nueva región, CloudTrail creará la misma ruta en la nueva región. En consecuencia, recibirá archivos de registro con la actividad de la API en la nueva región sin necesidad de realizar ninguna acción.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	rds-logging-enabled	Para facilitar el registro y el monitoreo en su entorno, asegúrese de que el registro de Amazon Relational Database Service (Amazon RDS) esté habilitado. Con el registro de Amazon RDS, puede capturar eventos tales como conexiones, desconexiones, consultas o tablas consultadas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	s3- bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporciona detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterm inada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	wafv2-logging-enabled	Para facilitar el registro y la supervisión en su entorno, habilite el registro AWS WAF (V2) en la web ACLs regional y global. AWS El registro WAF proporciona información detallada sobre el tráfico que analiza su ACL web. Los registros registran la hora en que AWS WAF recibió la solicitud de su AWS recurso, la información sobre la solicitud y una acción para la regla según la cual cada solicitud coincidió.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(h)	Registros de seguimiento	redshift-cluster-configuration-check	Para proteger los datos en reposo, asegúrese de que el cifrado esté activado en los clústeres de Amazon Redshift. También debe asegurarse de que las configuraciones necesarias se implementen en los clústeres de Amazon Redshift. El registro de auditoría debería habilitarse para proporcionar información acerca de las conexiones y las actividades de usuario en la base de datos. Esta regla requiere que se establezca un valor para clusterDbEncrypted (Config Default: TRUE) y LoggingEnabled (Config Default: TRUE). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(i)	Infraestructura de claves públicas	acm-certificate-expiration-check	Asegúrese de que la integridad de la red esté protegida asegurándose de que ACM emita los certificados X509. AWS Estos certificados deben ser válidos y estar vigentes. Esta regla requiere un valor para daysToExpiration (valor de prácticas recomendadas de seguridad AWS fundamentales: 90). El valor real debe reflejar las políticas de su organización.
3.1(i)	Infraestructura de claves públicas	alb-http-drop-invalid-encabezado activado	Asegúrese de que su Elastic Load Balancing (ELB) esté configurado para eliminar los encabezados http. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(i)	Infraestructura de claves públicas	alb-http-to-https-verificación de redireccionamiento	Para ayudar a proteger los datos en tránsito, asegúrese de que el equilibrador de carga de aplicació n redirija automátic amente las solicitud es HTTP no cifradas hacia HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1(i)	Infraestructura de claves públicas	api-gw-ssl-enabled	Asegúrese de que las etapas de la API de REST de Amazon API Gateway estén configuradas con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(i)	Infraestructura de claves públicas	opensearch-https-required	Como pueden existir datos confidenciales y, para ayudar a proteger los datos en tránsito, asegúrate de que HTTPS esté habilitado para las conexiones a tus dominios de Amazon OpenSearch Service.
3.1(i)	Infraestructura de claves públicas	elbv2- acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(i)	Infraestructura de claves públicas	elb-acm-certificate-required	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en tránsito, debe asegurarse de que el cifrado esté habilitado para su Elastic Load Balancing. Use AWS Certificate Manager para administrar, aprovisionar e implementar SSL/TLS certificados públicos y privados con AWS servicios y recursos internos.
3.1(i)	Infraestructura de claves públicas	elb-tls-https-listeners-solo	Asegúrese de que sus Elastic Load Balancers (ELBs) estén configurados con agentes de escucha SSL o HTTPS. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.1(i)	Infraestructura de claves públicas	redshift-require-tls-ssl	Asegúrese de que sus clústeres de Amazon Redshift requieran TLS/SSL cifrado para conectarse a los clientes de SQL. Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.
3.1(i)	Infraestructura de claves públicas	s3- bucket-ssl-requests-only	Para ayudar a proteger los datos en tránsito, asegúrese de que los buckets de Amazon Simple Storage Service (Amazon S3) requieran solicitudes para usar la capa de sockets seguros (SSL). Puesto que puede haber datos confidenciales, habilite el cifrado en tránsito para proteger esos datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Administración de vulnerabilidades	elastic-beanstalk-managed-updates-habilitado	La activación de las actualizaciones de plataforma gestionadas para un entorno de Amazon Elastic Beanstalk garantiza que se instalen las últimas correcciones, actualizaciones y características de la plataforma disponibles para el entorno. Mantenerse actualizado mediante la instalación de parches es una práctica recomendada para proteger los sistemas.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Administración de vulnerabilidades	rds-automatic-minor-version-habilitado para la actualización	Habilite las actualizaciones automáticas de las versiones secundarias en sus instancias de Amazon Relational Database Service (RDS) para garantizar que estén instaladas las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS, por sus siglas en inglés), que pueden incluir parches de seguridad y correcciones de errores.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Administración de vulnerabilidades	redshift-cluster-maintenancesettings-check	Esta regla garantiza que los clústeres de Amazon Redshift tengan la configuración preferida para su organización. En concreto, que tengan períodos de mantenimiento preferidos y períodos de retención automática de instantáneas para la base de datos. Esta regla requiere que configure el allowVersionUpgrade. El valor predeterminado es true. También te permite configurar de forma opcional el periodo preferred MaintenanceWindow (el predeterminado es sáb: 16:00 -sáb: 16:30) y el automated SnapshotRetention Periodo (el valor predeterminado es 1). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Administración de vulnerabilidades	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Administración de vulnerabilidades	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Administración de vulnerabilidades	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.3	Administración de vulnerabilidades	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5	Plan de gestión de crisis cibernéticas	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5	Plan de gestión de crisis cibernéticas	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5	Plan de gestión de crisis cibernéticas	ec2- -manager instance-managed-by-systems	Es posible realizar un inventario de las plataformas y aplicaciones de software de la organización mediante la administración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con Systems AWS Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, editor y versión, y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5	Plan de gestión de crisis cibernéticas	ec2- -check managedinstance-association-compliance-status	Use AWS Systems Manager Associations para ayudar con el inventario de las plataformas y aplicaciones de software dentro de una organización. AWS Systems Manager asigna un estado de configuración a las instancias administradas y le permite establecer líneas base de los niveles de parches del sistema operativo, las instalaciones de software, las configuraciones de las aplicaciones y otros detalles sobre su entorno.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.5	Plan de gestión de crisis cibernéticas	ec2- -check managedinstance-patch-compliance-status	Habilite esta regla para ayudar a identificar y documentar las vulnerabilidades de Amazon Elastic Compute Cloud (Amazon EC2). La regla comprueba si los parches de instancias Amazon EC2 cumplen con los requisitos de las políticas y procedimientos de su organización en AWS Systems Manager.
3.9	Evaluación de riesgos de TI	annual-risk-assessment-performed (verificación del proceso)	Realice una evaluación anual de los riesgos de su organización. Las evaluaciones de riesgos pueden ayudar a determinar la probabilidad y el impacto de los riesgos y and/or vulnerabilidades identificados que afectan a una organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
3.12	Formación	security-awareness-program-exists (verificación del proceso)	Establezca y mantenga un programa de concienciación sobre la seguridad para su organización. Los programas de concienciación sobre la seguridad enseñan al personal a proteger la organización frente a diversas infracciones o incidentes de seguridad.
4.4(g)	Análisis de fraudes: análisis de transacciones sospechosas, malversación de fondos, robo o sospecha de blanqueo de dinero, apropiación indebida de activos, manipulación de registros financieros, etc. El requisito normativo de denunciar el fraude al RBI debe estar impulsado por el sistema.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendizaje automático para identificar actividades inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	clb-multiple-az	Elastic Load Balancing (ELB) distribuye automáticamente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibilidad. Para garantizar una alta disponibilidad, asegúrese de que su ELB tenga instancias registradas de varias zonas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantiza r una alta disponibi lidad, asegúrese de que su ELB tenga instancias registrad as de varias zonas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	lambda-vpc-multi-az-comprobar	Si su función AWS Lambda está configurada para conectarse a una nube privada virtual (VPC) de su cuenta, implemente la función AWS Lambda en al menos dos zonas de disponibilidad diferentes para asegurarse de que su función esté disponibl e para procesar eventos en caso de una interrupción del servicio en una sola zona.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	rds-instance-deletion-protection-habilitada	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitada la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	s3- bucket-default-loc k-enabled	Asegúrese de que su bucket de Amazon Simple Storage Service (Amazon S3) tenga el bloqueo habilitado de forma predeterminada. Puesto que puede haber datos confidenc iales en reposo en los buckets de S3, habilite el bloqueo de objetos en reposo para protegerlos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultane idad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	lambda-dlq-check	Active esta regla para ayudar a notificar al personal correspon diente mediante Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) cuando una función falle.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	beanstalk-enhanced-health-reporting-habilitado	AWS Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación. Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	ebs-optimized-instance	Una instancia optimizada en Amazon Elastic Block Store (Amazon EBS) proporciona capacidad adicional y dedicada para las operaciones de Amazon EBS. I/O Esta optimización proporciona el rendimiento más eficiente para sus volúmenes de EBS al minimizar la contención entre I/O las operaciones de Amazon EBS y el resto del tráfico de su instancia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(h)	Análisis de la capacidad y el rendimiento de los sistemas de seguridad de TI.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(i)	Notificación de incidentes, de su impacto y de las medidas adoptadas para que no se repitan tales eventos en el futuro.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
4.4(i)	Notificación de incidentes, de su impacto y de las medidas adoptadas para que no se repitan tales eventos en el futuro.	guardduty-non-archived-findings	Amazon te GuardDuty ayuda a entender el impacto de un incidente mediante la clasificación de los hallazgos por gravedad: baja, media y alta. Puede utilizar estas clasificaciones para determinar las estrategias y prioridades de corrección. Esta regla le permite configurar de forma opcional los valores daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) y daysHighSev (Config Default: 1) para los hallazgos no archivados, según lo exijan las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	aurora-resources-protected-by-plan de respaldo	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Aurora formen parte de un plan de AWS respaldo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	cmk-backing-key-rotation-habilitado	Habilite la rotación de claves para garantizar que las claves se roten una vez que hayan alcanzado el final de su período criptográfico.
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	ec2- -plan resources-protected-by-backup	Para facilitar los procesos de respaldo de datos, asegúrese de que sus recursos de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) formen parte de un plan de respaldo. AWS AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	elasticache-redis-cluster-automatic-verificación de respaldo	Cuando las copias de seguridad automáticas están habilitadas, Amazon ElastiCache crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerará la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	fsx-resources-protected-by-plan de respaldo	Para facilitar los procesos de backup de datos, asegúrate de que tus sistemas de FSx archivos de Amazon formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relational Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
6.3	NBFCs considerarán la necesidad de establecer los sitios de respaldo necesarios para sus sistemas empresariales y centros de datos críticos.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	dynamodb-autoscaling-enabled	El escalado automático de Amazon DynamoDB AWS usa el servicio Application Auto Scaling para ajustar la capacidad de rendimiento aprovisionada para que responda automáticamente a los patrones de tráfico reales. Esto permite que una tabla o un índice secundario global aumente su read/write capacidad aprovisionada para gestionar los aumentos repentinos de tráfico, sin limitaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	elb-cross-zone-load-habilitado para el equilibrio	Habilite el equilibrio de carga entre zonas para sus Elastic Load Balancers (ELBs) para ayudar a mantener la capacidad y la disponibilidad adecuadas. El equilibrio de carga entre zonas reduce la necesidad de mantener automátic amente cantidade s equivalentes de instancias en cada zona de disponibilidad habilitada. También mejora la capacidad de la aplicación para gestionar la pérdida de una o más instancias.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	elb-deletion-protection-enabled	Esta regla garantiza que Elastic Load Balancing tenga habilitada la protección contra borrado. Utilice esta característica para evitar que el equilibrador de carga se elimine de forma accidental o malintencionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	clb-multiple-az	Elastic Load Balancing (ELB) distribuye automáticamente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibilidad. Para garantizar una alta disponibilidad, asegúrese de que su ELB tenga instancias registradas de varias zonas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuye automátic amente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una zona de disponibi lidad. Para garantiza r una alta disponibi lidad, asegúrese de que su ELB tenga instancias registrad as de varias zonas de disponibilidad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	lambda-vpc-multi-az-comprobar	Si su función AWS Lambda está configurada para conectarse a una nube privada virtual (VPC) de su cuenta, implemente la función AWS Lambda en al menos dos zonas de disponibilidad diferentes para asegurarse de que su función esté disponibl e para procesar eventos en caso de una interrupción del servicio en una sola zona.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	rds-instance-deletion-protection-habilitada	Asegúrese de que las instancias de Amazon Relational Database Service (Amazon RDS) tengan habilitad a la protección contra borrado. Utilice la protección contra borrado para evitar que las instancias de Amazon RDS se eliminen de forma accidental o malintenc ionada, lo que puede provocar la pérdida de disponibilidad de sus aplicaciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	rds-multi-az-support	La compatibilidad con las zonas de disponibilidad múltiples (Multi-AZ) de Amazon Relational Database Service (Amazon RDS) permite mejorar la disponibilidad y durabilidad de las instancias de bases de datos. Cuando aprovisiona una instancia de base de datos Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cada zona de disponibilidad se ejecuta en su propia infraestructura independiente y físicamente distinta, y está diseñada para ser altamente fiable. En caso de que se produzca un fallo en

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			la infraestructura, Amazon RDS realiza una conmutación por error automátic a a la estación en espera para que pueda reanudar las operaciones de la base de datos en cuanto se complete la conmutación por error.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	vpc-vpn-2-tunnels-up	Se pueden implementar túneles Site-to-Site VPN redundantes para cumplir con los requisitos de resiliencia. Utiliza dos túneles para garantizar la conectividad en caso de que una de las conexiones Site-to-Site VPN no esté disponible. Para protegerse contra la pérdida de conectividad, en caso de que su pasarela de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su Amazon Virtual Private Cloud (Amazon VPC) y a su puerta de enlace privada virtual mediante una segunda pasarela de cliente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	autoscaling-group-elb-healthcheck-obligatorio	Las revisiones de estado de Elastic Load Balancer (ELB) para los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) permiten mantener la capacidad y disponibilidad adecuadas. De forma periódica, el equilibrador de carga envía pings, intenta establecer conexiones o envía solicitudes para probar el estado de las instancias de Amazon EC2 en un grupo de escalado automático. Si una instancia no informa, el tráfico se envía a una nueva instancia de Amazon EC2.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	dynamodb-throughput-limit-check	Active esta regla para asegurarse de que la capacidad de rendimiento aprovisionada se compruebe en las tablas de Amazon DynamoDB. Esta es la cantidad de read/write actividad que puede soportar cada mesa. DynamoDB utiliza esta información para reservar recursos del sistema suficientes para satisfacer sus necesidades de rendimiento. Esta regla genera una alerta cuando el rendimiento se acerca al límite máximo de la cuenta de un cliente. Esta regla le permite configurar opcionalmente los parámetros de RCUThreshold porcentaje de cuenta (Config Default: 80) y WCUThreshold Percentage de cuenta (Config Default:

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			80). Los valores reales deben reflejar las políticas de su organización.
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	ec2- instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de inteligencia sobre amenazas. Estas incluyen listas de datos maliciosos IPs y de aprendiza je automático para identificar actividad es inesperadas, no autorizadas y maliciosas en su entorno de AWS nube.
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	lambda-concurrency-check	Esta regla garantiza que se establezcan los límites máximos y mínimos de simultane idad de una función Lambda. Esto puede ayudar a la hora de establecer el número de solicitudes de referencia que la función atiende en un momento dado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	rds-enhanced-monitoring-enabled	Habilite Amazon Relational Database Service (Amazon RDS) para monitorear la disponibilidad de Amazon RDS. Esto proporciona información detallada del estado de las instancias de bases de datos de Amazon RDS. Cuando el almacenamiento de Amazon RDS utiliza más de un dispositivo físico subyacente, el monitoreo mejorado recopila los datos de cada dispositivo. Además, cuando la instancia de base de datos de Amazon RDS se ejecuta en una implementación Multi-AZ, se recopilan los datos de cada dispositivo del host secundario y las métricas del host secundario.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.1	Los sistemas de TI deberían escalarse verticalmente progresivamente a medida que aumenten el tamaño y la complejidad de las operaciones de NBFC.	securityhub-enabled	AWS Security Hub ayuda a monitorea r el personal, las conexiones, los dispositivos y el software no autorizad os. AWS Security Hub agrupa, organiza y prioriza las alertas de seguridad, o hallazgos, de varios servicios. AWS Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer y AWS Firewall Manager y Partner Solutions. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	s3- bucket-policy-gran tee-check	Administre el acceso a la AWS nube habilitando s3_ bucket_policy_gran tee_check. Esta regla comprueba que el acceso otorgado por el bucket de Amazon S3 esté restringido por cualquiera de AWS los principales, usuarios federados , principales de servicio, direccion es IP o Amazon Virtual Private Cloud (Amazon VPC) que usted proporcione. IDs
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	dms-replication-not-public	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de replicaci ón del DMS. Las instancias de replicaci ón de DMS pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	ebs-snapshot-public-restorable-comprobar	Gestione el acceso a la AWS nube asegurándose de que las instantáneas de EBS no se puedan restaurar públicame nte. Las instantán eas de volumen de EBS pueden contener información confidenc ial y dichas cuentas requieren control de acceso.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	ec2- instance-no-public-ip	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	elasticsearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch OpenSearch Service (Service) estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de OpenSearch servicio dentro de una Amazon VPC permite una comunicac ión segura entre el OpenSearch Servicio y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	emr-master-no-public-IP	Gestione el acceso a la AWS nube asegurándose de que no se pueda acceder públicamente a los nodos maestros del clúster de Amazon EMR. Los nodos maestros del clúster de Amazon EMR pueden contener información confidenc ial y dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	ec2- instances-in-vpc	Implemente instancia s de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la AWS nube. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			Amazon VPC para gestionar correctam ente el acceso.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	internet-gateway-a uthorized-vpc-solo	Gestione el acceso a los recursos de la AWS nube asegurándose de que las puertas de enlace de Internet solo estén conectadas a Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidirecci onal a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	lambda-function-public-access-prohibido	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para una comunicac ión segura entre una función y otros servicios de la Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece de forma segura dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctamente el acceso, las funciones de AWS Lambda

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			deben asignarse a una VPC.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	rds-instance-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	rds-snapshots-public-prohibited	Gestione el acceso a los recursos en la AWS nube asegurándose de que las instancias de Amazon Relationa l Database Service (Amazon RDS) no sean públicas. Las instancias de base de datos de Amazon RDS pueden contener información confidenc ial y principios. Además, dichas cuentas requieren control de acceso.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	redshift-cluster-public-access-comprobar	Gestione el acceso a los recursos en la AWS nube asegurándose de que los clústeres de Amazon Redshift no sean públicos. Los clústeres de Amazon Redshift pueden contener informaci ón confidencial y principios. Además dichas cuentas requieren control de acceso.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	restricted-common-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPort1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	s3- -bloques-periódicos account-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar opcionalmente los restrictPublicBuckets parámetros ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) y (Config Default: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	s3- bucket-public-read -prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	s3- bucket-public-writ e-prohibited	Gestione el acceso a los recursos de la AWS nube permitien do que solo los usuarios, procesos y dispositivos autorizad os accedan a los depósitos de Amazon Simple Storage Service (Amazon S3). La administr ación del acceso debe ser coherente con la clasificación de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	sagemaker-notebook -no-direct-acceso a internet	Gestione el acceso a los recursos en la AWS nube asegurándose de que las SageMaker libretas de Amazon no permitan el acceso directo a Internet. Al impedir el acceso directo a internet, puede evitar que usuarios no autorizad os accedan a los datos confidenciales.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	vpc-default-security-group-cerrado	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a gestionar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos. AWS Restringir todo el tráfico en el grupo de seguridad predeterm inado ayuda a restringir el acceso remoto a los recursos. AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos de la AWS nube asegurándose de que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integridad y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizad os para garantiza r que las claves de acceso de IAM se roten según la política de la organización. Cambiar las claves de acceso de forma habitual es una práctica recomenda da de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven compromet idas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	emr-kerberos-enabled	Los permisos y autorizaciones de acceso se pueden administr ar e incorporar con los principios de privilegio mínimo y separación de funciones al habilitar Kerberos para los clústeres de Amazon EMR. En Kerberos, los servicios y los usuarios que deben autenticarse se denominan entidades principales. Las entidades principal es existen dentro de un ámbito de Kerberos. Dentro de ese ámbito, un servidor de Kerberos se conoce como el centro de distribuc ión de claves (KDC). Este proporciona un medio para que las entidades principal es se autentiquen. El KDC se autentica emitiendo tickets de autenticación. El

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			KDC mantiene una base de datos de las entidades principales dentro de su ámbito, sus contraseñas y otros datos administrativos sobre cada una de las entidades principales.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	iam-group-has-users-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegios mínimos y separación de funciones en los permisos y autorizaciones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	autoscaling-launch -config-public-ip- deshabilitado	Si configura las interfaces de red con una dirección IP pública, se puede acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus aplicaciones o servidores.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	ec2- instance-profile-a ttached	Los perfiles de instancias de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	ecs-task-definition-nonroot-usuario	Para ayudar a implementar el principio de privilegio mínimo, asegúrese de designar a un usuario que no sea raíz para acceder a las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS).

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	efs-access-point-enforce-directorio raíz	La aplicación de un directorio raíz para un punto de acceso de Amazon Elastic File System (Amazon EFS) ayuda a restringir el acceso a los datos al garantizar que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	efs-access-point-e nforce-identidad de usuario	Para ayudar a implementar el principio de privilegios mínimos, asegúrese de que la aplicació n por parte de los usuarios esté habilitad a en su Amazon Elastic File System (Amazon EFS). Cuando está habilitad o, Amazon EFS reemplaza el usuario y el grupo IDs del cliente de NFS por la identidad configura da en el punto de acceso para todas las operaciones del sistema de archivos y solo permite el acceso a esta identidad de usuario forzada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	s3- bucket-acl-prohibi ted	Esta regla comprueba si las listas de control de acceso (ACLs) se utilizan para el control de acceso en los buckets de Amazon S3. ACLs son mecanismos de control de acceso heredados para los buckets de Amazon S3 anteriores a Identity and Access Management (IAM) (AWS Identity and Access Management) (IAM). En lugar de ello ACLs, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	s3-: prohibido bucket-level-public-access	Gestione el acceso a los recursos en la AWS nube asegurándose de que no se pueda acceder públicamente a los depósitos de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer informaci ón sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	subnet-auto-assign-public-ip deshabilitado	Gestione el acceso a la AWS nube asegurándose de que a las subredes de Amazon Virtual Private Cloud (VPC) no se les asigne automáticamente una dirección IP pública. Las instancia s de Amazon Elastic Compute Cloud (EC2) que se lanzan en subredes que tienen este atributo habilitad o tienen una dirección IP pública asignada a su interfaz de red principal.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	iam-root-access-key-comprobar	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de AWS Identity and Access Managemen t (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de AWS para ayudar a incorporar el principio de funcionalidad mínima.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	iam-user-mfa-enabled	Activa esta regla para restringir el acceso a los recursos de la AWS nube. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas compromet idas exigiendo la MFA a los usuarios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	mfa-enabled-for-iam-acceso a la consola	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	root-account-hardware-mfa-habilitado	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA de hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	opensearch-in-vpc-only	Gestione el acceso a la AWS nube asegurándose de que los dominios de Amazon OpenSearch Service estén dentro de una Amazon Virtual Private Cloud (Amazon VPC). Un dominio de Amazon OpenSearch Service dentro de una Amazon VPC permite una comunicación segura entre Amazon OpenSearch Service y otros servicios de la Amazon VPC sin necesidad de una pasarela de Internet, un dispositivo NAT o una conexión VPN.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñas bien definida.	root-account-mfa-enabled	Gestione el acceso a los recursos en la AWS nube asegurándose de que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir MFA para el usuario root, puede reducir los incidentes de amenazas. Cuentas de AWS

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	secretsmanager-rot ation-enabled-check	Esta regla garantiza que AWS los secretos de Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencial mente, reducir el impacto sobre la empresa si el secreto se desvela.
8.I	Aspectos básicos de seguridad, como los controles de acceso físicos/lógicos y una política de contraseñ as bien definida.	secretsmanager-sch eduled-rotation-su ccess-comprobar	Esta regla garantiza que AWS los secretos de Secrets Manager se hayan distribui do correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.II	Un rol de usuario bien definido.	iam-group-has-users-comprobar	AWS Identity and Access Managemen t (IAM) puede ayudarle a incorpora r los principios de privilegios mínimos y separación de funciones en los permisos y autorizac iones de acceso, garantizando que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegios mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.II	Un rol de usuario bien definido.	iam-no-inline-policy-comprobar	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política integrada para controlar el acceso a los sistemas y activos. AWS recomiend a utilizar políticas gestionadas en lugar de políticas integradas. Las políticas administr adas permiten la reutilización, el control de versiones , la reversión y la delegación de la administración de permisos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.II	Un rol de usuario bien definido.	iam-password-policy	Las identidades y las credenciales se emiten, administr an y verifican en función de la política de contraseñas de IAM de la organizac ión. Cumplen o superan los requisito s establecidos en la norma NIST SP 800-63 y en el estándar AWS fundamental de mejores prácticas de seguridad para la seguridad de las contraseñ as. Esta regla le permite configura r opcionalmente RequireUppercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireLowercaseCh aracters (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			), RequireSy mbols (valor de las mejores prácticas de seguridad AWS fundament ales: verdadero), RequireNu mbers (valor de las mejores prácticas de seguridad AWS AWS fundament ales: verdadero), MinimumPa sswordLength (valor de las mejores prácticas de seguridad AWS fundamentales: 14), PasswordReusePreve ntion (valor de las mejores prácticas de seguridad AWS fundamentales: 24) y MaxPasswo rdAge (valor de las mejores prácticas de seguridad fundament ales: 90) para su IAM La política de contraseñas. Los valores reales deben reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.II	Un rol de usuario bien definido.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) puede ayudarlo a incorporar los principios del mínimo privilegio y la separación de funciones en los permisos y autorizaciones de acceso, impidiendo que las políticas contengan «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*». Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.II	Un rol de usuario bien definido.	iam-user-group-membership-comprobar	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.II	Un rol de usuario bien definido.	iam-user-no-policies-comprobar	Esta regla garantiza que las políticas de AWS Identity and Access Managemen t (IAM) se adjunten únicamente a grupos o funciones para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunid ades de que una identidad reciba o conserve demasiados privilegios.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.II	Un rol de usuario bien definido.	iam-user-unused-credentials-comprobar	AWS Identity and Access Management (IAM) puede ayudarlo con los permisos y autorizaciones de acceso comprobando las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican estas credenciales no utilizadas, debe deshabilitar la opción de and/or eliminar las credenciales, ya que esto podría infringir el principio del privilegio mínimo. Esta regla requiere que establezcas un valor en la maxCredentialUsage Edad (Config Default: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.III	Un concepto de creación-comprobación para reducir el riesgo de errores y usos indebidos y garantizar la fiabilidad de los datos/información.	s3- bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	db-instance-backup-enabled	La característica de copia de seguridad de Amazon RDS crea copias de seguridad de sus bases de datos y registros de transacciones. Amazon RDS crea automáticamente una instantánea de volumen de almacenamiento de la instancia de base de datos y realiza una copia de seguridad de toda la instancia. El sistema le permite establecer períodos de retención específicos para cumplir con sus requisitos de resiliencia.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	dynamodb-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	dynamodb-pitr-enabled	Active esta regla para comprobar que se haya realizado una copia de seguridad de la información. También mantiene las copias de seguridad al garantizar que la point-in-time recuperación esté habilitada en Amazon DynamoDB. La recuperación mantiene copias de seguridad continuas de la tabla durante los últimos 35 días.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	ebs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de backup. AWS AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	efs-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus sistemas de archivos Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	elasticache-redis-cluster-automatic-verificación de copias de seguridad	Cuando las copias de seguridad automátic as están habilitadas, Amazon ElastiCac he crea una copia de seguridad del clúster a diario. La copia de seguridad se puede conservar durante el número de días que especifique su organización. Las copias de seguridad automáticas pueden ayudarle a protegers e frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	rds-in-backup-plan	Para facilitar los procesos de backup de datos, asegúrese de que sus instancias de Amazon Relationa l Database Service (Amazon RDS) formen parte de un AWS plan de backup. AWS Backup es un servicio de respaldo totalmente administr ado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisito s empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	s3- bucket-replication-enabled	Con la replicación entre regiones (CRR) de Amazon Simple Storage Service (Amazon S3) se puede mantener la capacidad y la disponibilidad adecuadas. La CRR permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica para garantizar la disponibilidad de los datos.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	redshift-backup-enabled	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus clústeres de Amazon Redshift tengan instantáneas automatizadas. Cuando las instantáneas automatizadas están habilitadas para un clúster, Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	backup-plan-min-frequency-and-min-retention-check	Para ayudar con los procesos de respaldo de datos, asegúrese de que su plan de AWS respaldo esté configurado para una frecuencia y retención mínimas. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite configurar los parámetros requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) y requiredFrequencyUnit (Config

ID de control	Descripción del control	AWS Regla de configuración	Directrices
			default: days). El valor real debe reflejar los requisitos de su organización.
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	backup-recovery-point-manual-eliminación-deshabilitada	Asegúrese de que sus puntos AWS de recuperación de Backup tengan adjunta una política basada en los recursos que impida la eliminación de los puntos de recuperación. El uso de una política basada en los recursos para evitar eliminar puntos de recuperación ayuda a evitar que se eliminen de forma accidental o intencionada.

ID de control	Descripción del control	AWS Regla de configuración	Directrices
8.IX	Disposición para la copia de seguridad de los datos con pruebas periódicas.	backup-recovery-point-minimum-control de retención	Para facilitar los procesos de backup de datos, asegúrese de que sus puntos AWS de recuperación de Backup tengan establecido un período de retención mínimo. AWS Backup es un servicio de respaldo totalmente administrado con una solución de respaldo basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad. Esta regla le permite establecer el parámetro requiredRetentionDays (configuración predeterminada: 35). El valor real debe reflejar los requisitos de su organización.

Plantilla

La plantilla está disponible en GitHub: Mejores prácticas operativas para el RBI MD-ITF.

Prácticas operativas recomendadas para los servicios de seguridad, identidad y conformidad

Este paquete de conformidad contiene AWS Config reglas basadas en los servicios de seguridad, identidad y cumplimiento. Para obtener más información, consulte Seguridad, identidad y conformidad en AWS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para los servicios de seguridad, identidad y cumplimiento.

Prácticas operativas recomendadas para soluciones sin servidor

Este paquete de conformidad contiene AWS Config reglas basadas en soluciones sin servidor. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Prácticas recomendadas operativas para sistemas sin servidor.

Prácticas operativas recomendadas para servicios de almacenamiento

Este paquete de conformidad contiene AWS Config reglas basadas en los servicios de almacenamiento. Para obtener más información, consulta Cloud Storage en AWS. Para ver una lista de todas las reglas administradas compatibles AWS Config, consulta la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Mejores prácticas operativas para los servicios de almacenamiento.

Prácticas operativas recomendadas para el SWIFT CSP

Los paquetes de conformidad proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear comprobaciones de control de seguridad, operativas o de optimización de costos mediante reglas de AWS Config administradas o personalizadas y acciones correctivas de AWS Config. Los paquetes de conformidad, como plantillas de ejemplo, no están diseñados para garantizar plenamente el cumplimiento de una norma de gobernanza o de conformidad específicas. Usted debe evaluar si su uso de los servicios cumple con los requisitos legales y normativos aplicables.

A continuación, se proporciona un ejemplo de asignación entre el Programa de Seguridad de los Clientes de SWIFT (SWIFT CSP) y las reglas de AWS Config administradas. Cada regla de AWS Config se aplica a un recurso de AWS específico que está relacionado con uno o más controles del SWIFT CSP. Un control del SWIFT CSP puede estar relacionado con varias reglas de AWS Config. Consulte la siguiente tabla para obtener más detalles y orientación relacionados con estas asignaciones.

ID de control	Regla de AWS Config	Directrices
1.1	ec2-instance-managed-by-systems-manager	Se puede realizar un inventario de las aplicaciones y plataformas de software de la organización mediante la administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager. Use AWS Systems Manager para proporcionar configuraciones detalladas del sistema, niveles de parches del sistema operativo, nombre y tipo de servicios, instalaciones de software, nombre de la aplicación, publicador y

ID de control	Regla de AWS Config	Directrices
		versión, y otros detalles sobre su entorno.
1.1	ec2-instance-no-public-ip	Gestione el acceso a la nube de AWS de manera que se garantice que no se puede acceder públicamente a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las instancias de Amazon EC2 pueden contener información confidencial y dichas cuentas requieren control de acceso.
1.1	ec2-no-amazon-key-pair	Comprueba si las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en ejecución se lanzan con pares de claves de Amazon. Esto puede ayudar a reducir el riesgo de que las credencia les se vean comprometidas. Aún se puede acceder a las instancias de Amazon EC2 sin pares de claves mediante el administrador de sesiones o una conexión SSH basada en el navegador, a través de la consola de AWS.

ID de control	Regla de AWS Config	Directrices
1.1	ec2-instances-in-vpc	Implemente instancias de Amazon Elastic Compute Cloud (Amazon EC2) dentro de una Amazon Virtual Private Cloud (Amazon VPC) para permitir una comunicación segura entre una instancia y otros servicios dentro de la Amazon VPC, sin necesidad de utilizar una puerta de enlace de internet, un dispositivo NAT ni una conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Asigne instancias de Amazon EC2 a una Amazon VPC para gestionar correctamente el acceso.

ID de control	Regla de AWS Config	Directrices
1.1	vpc-default-security-group-closed	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar filtros con estado del tráfico de red de entrada y salida a los recursos de AWS. Restringir todo el tráfico en el grupo de seguridad predeterminado ayuda a restringir el acceso remoto a los recursos de AWS.
1.1	vpc-network-acl-unused-check	Esta regla garantiza que se utilicen las listas de control de acceso a la red de Amazon Virtual Private Cloud (VPC). El monitoreo de las listas de control de acceso a la red no utilizadas puede ayudar a realizar un inventario y una gestión precisos del entorno.

ID de control	Regla de AWS Config	Directrices
1.1	vpc-sg-open-only-to-authorized-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Al restringir el acceso a los recursos dentro de un grupo de seguridad desde internet (0.0.0.0/0), se puede controlar el acceso remoto a los sistemas internos.

ID de control	Regla de AWS Config	Directrices
1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y la separación de funciones con permisos y autorizaciones de acceso, lo que impide que las políticas incluyan acciones bloqueadas en todas las claves del AWS Key Management Service. Tener más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones. Esta regla le permite establecer el parámetro blockedActionsPatterns. (Valor de las prácticas recomendadas de seguridad básica de AWS: kms:Decrypt, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
1.2	iam-group-has-users-check	AWS Identity and Access Management (IAM) puede ayudarle a incorporar los principios de privilegio mínimo y separación de funciones con permisos y autorizaciones de acceso al garantizar que los grupos de IAM tengan al menos un usuario. Una forma de incorporar privilegi os mínimos es colocar a los usuarios en grupos en función de los permisos o funciones laborales asociados.

ID de control	Regla de AWS Config	Directrices
1.2	iam-inline-policy-blocked-kms-actions	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada que permita acciones bloqueadas en todas las claves de AWS Key Management Service. AWS recomienda que utilice políticas administr adas en lugar de políticas insertadas. Las políticas administradas permiten la reutilización, el control de versiones, la reversión y la delegación de la administr ación de permisos. Esta regla le permite establecer el parámetro blockedActionsPatt erns. (Valor de las prácticas recomendadas de seguridad básica de AWS: kms:Decry pt, kms:ReEncryptFrom). Los valores reales deben reflejar las políticas de su organizac ión.

ID de control	Regla de AWS Config	Directrices
1.2	iam-no-inline-policy-check	Asegúrese de que un usuario de AWS Identity and Access Management (IAM), un rol de IAM o un grupo de IAM no tengan una política insertada para controlar el acceso a los sistemas y activos. AWS recomienda que se utilicen políticas administradas en lugar de políticas insertada s. Las políticas administr adas permiten la reutilización, el control de versiones, la reversión y la delegación de la administración de permisos.
1.2	iam-user-no-policies-check	Esta regla garantiza que las políticas de AWS Identity and Access Management (IAM) se adjunten solo a grupos o roles para controlar el acceso a los sistemas y activos. La asignación de privilegios en el nivel de grupo o rol ayuda a reducir las oportunidades de que una identidad reciba o conserve demasiados privilegi os.

ID de control	Regla de AWS Config	Directrices
1.2	restricted-ssh	Los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) pueden ayudar a administrar el acceso a la red al proporcionar un filtrado continuo del tráfico de red de entrada y salida a los recursos de AWS. Al no permitir el tráfico de entrada (o el tráfico remoto) desde 0.0.0.0/0 al puerto 22 en sus recursos, podrá restringir el acceso remoto.
1.2	nacl-no-unrestricted-ssh-rdp	El acceso a los puertos de administración remota de servidores de las listas de control de acceso a la red (NACL), como el puerto 22 (SSH) y el puerto 3389 (RDP), no debe ser de acceso público, ya que esto puede permitir el acceso no deseado a los recursos de la VPC.

ID de control	Regla de AWS Config	Directrices
1.2	s3-bucket-acl-prohibited	Esta regla comprueba si las listas de control de acceso (ACL) se utilizan para el control de acceso en los buckets de Amazon S3. Las ACL son mecanismos de control de acceso heredados para buckets de Amazon S3 que sean anteriores a AWS Identity and Access Management (IAM). En lugar de las ACL, se recomiend a utilizar políticas de IAM o políticas de bucket de S3 para gestionar más fácilmente el acceso a los buckets de S3.

ID de control	Regla de AWS Config	Directrices
1.2	s3-bucket-logging-enabled	El registro de acceso al servidor de Amazon Simple Storage Service (Amazon S3) proporciona un método para monitorear la red en busca de posibles eventos de ciberseguridad. Los eventos se monitorean mediante la captura detallada de las solicitudes realizadas a un bucket de Amazon S3. Cada registro de acceso proporcio na detalles sobre una única solicitud de acceso. Los detalles incluyen el solicitan te, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si procede.

ID de control	Regla de AWS Config	Directrices
1.2	s3-bucket-policy-grantee-check	Gestione el acceso a la nube de AWS habilitando s3_bucket_policy_grantee_check. Esta regla comprueba que el acceso concedido por el bucket de Amazon S3 esté restringido por cualquiera de las entidades principales de AWS, usuarios federados, entidades principales de servicio, direcciones IP o ID de Amazon Virtual Private Cloud (Amazon VPC) que proporcione.

ID de control	Regla de AWS Config	Directrices
1.2	sns-topic-message-delivery-notification-enabled	Para ayudarle a cumplir los requisitos de registro en su entorno, asegúrese de activar las notificaciones de estado de entrega para los temas de Amazon Simple Notificat ion Service (Amazon SNS). Registrar el estado de entrega de los mensajes ayuda a proporcionar una mejor visión operativa, compuesta por elementos como los siguiente s: saber si un mensaje se ha entregado al punto de conexión de Amazon SNS, identificar la respuesta enviada desde el punto de conexión de Amazon SNS a Amazon SNS y determina r el tiempo de permanenc ia del mensaje (el tiempo transcurrido entre la fecha de publicación y el instante previo a su entrega a un punto de conexión de Amazon SNS).

ID de control	Regla de AWS Config	Directrices
1.4	internet-gateway-authorized-vpc-only	Gestione el acceso a recursos en la nube de AWS de manera que garantice que las puertas de enlace de Internet solo se conecten a la Amazon Virtual Private Cloud (Amazon VPC) autorizada. Las puertas de enlace de Internet permiten el acceso bidireccional a internet desde y hacia la Amazon VPC, lo que puede provocar un acceso no autorizado a los recursos de Amazon VPC.

ID de control	Regla de AWS Config	Directrices
1.4	restricted-common-ports	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que los puertos comunes estén restringidos en los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2). No restringir el acceso a los puertos a solamente fuentes fiables puede afectar a la disponibilidad, integrida d y confidencialidad de los sistemas. Esta regla le permite configurar de forma opcional los parámetros blockedPo rt1 a blockedPort5 (valores predeterminados de Config: 20,21,3389,3306,4333). Los valores reales deben reflejar las políticas de su organizac ión.
1.4	lambda-function-public-acce ss-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que se garantice que no se pueda acceder públicamente a las funciones de AWS Lambda. El acceso público puede degradar la disponibilidad de los recursos.

ID de control	Regla de AWS Config	Directrices
1.4	s3-account-level-public-access-blocks-periodic	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público. Esta regla le permite configurar de forma opcional los parámetros ignorePublicAcls (valor predeterminado de Config: True), blockPublicPolicy (valor predeterminado de Config: True), blockPublicAcls (valor predeterminado de Config: True) y restrictPublicBuckets (valor predeterminado de Config: True). Los valores reales deben reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
1.4	s3-bucket-level-public-access-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que no se pueda acceder públicamente a buckets de Amazon Simple Storage Service (Amazon S3). Esta regla ayuda a proteger los datos confidenciales de usuarios remotos no autorizados al impedir el acceso público en el nivel del bucket.
1.4	s3-bucket-public-read-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.

ID de control	Regla de AWS Config	Directrices
1.4	s3-bucket-public-write-prohibited	Gestione el acceso a los recursos en la nube de AWS de manera que solo permita a los usuarios, procesos y dispositivos autorizados acceder a buckets de Amazon Simple Storage Service (Amazon S3). La administración del acceso debe ser coherente con la clasificación de los datos.
1.4	ssm-document-not-public	Asegúrese de que los documentos de AWS Systems Manager (SSM) no sean públicos, ya que esto podría permitir el acceso no deseado a los documentos de SSM. Un documento de SSM público puede exponer información sobre su cuenta, sus recursos y sus procesos internos.

ID de control	Regla de AWS Config	Directrices
2.3	ec2-imdsv2-check	Asegúrese de que el método Servicio de metadatos de instancias versión 2 (IMDSv2) esté habilitado para ayudar a proteger el acceso y el control de los metadatos de instancia de Amazon Elastic Compute Cloud (Amazon EC2). El método IMDSv2 utiliza controles basados en sesiones. IMDSv2 permite implementar controles para restringir los cambios en los metadatos de la instancia.
2.3	ec2-instance-multiple-eni-check	Esta regla comprueba si las instancias de Amazon Elastic Compute Cloud (Amazon EC2) tienen varios ENI. Tener varios ENI puede provocar instancias de doble host, es decir, instancias que tienen varias subredes. Esto puede añadir complejidad a la seguridad de la red e introducir rutas y accesos a la red no deseados.

ID de control	Regla de AWS Config	Directrices
2.3	ec2-token-hop-limit-check	Asegúrese de que la respuesta HTTP PUT del servicio de metadatos de instancias (IMDS) esté restringida a la instancia de Amazon Elastic Compute Cloud (Amazon EC2). Con IMDSv2, la respuesta PUT que contiene el token secreto de forma predeterminada no puede viajar fuera de la instancia, ya que el límite de saltos de respuesta de metadatos está establecido en 1 (valor predeterminado de Config). Si este valor es superior a 1, el token puede salir de la instancia EC2.
2.3	ec2-volume-inuse-check	Esta regla garantiza que los volúmenes de Amazon Elastic Block Store que están adjuntos a instancias de Amazon Elastic Compute Cloud (Amazon EC2) estén marcados para su eliminaci ón al finalizar una instancia . Si un volumen de Amazon EBS no se elimina al finalizar la instancia a la que está asociado, podría infringir el concepto de funcionalidad mínima.

ID de control	Regla de AWS Config	Directrices
2.3	account-part-of-organizations	La administración centralizada de Cuentas de AWS dentro de AWS Organizations contribuye a garantizar la conformidad de las cuentas. La falta de gobernanza centralizada de las cuentas puede provocar incoherencias en las configuraciones de cuentas, lo que puede exponer los recursos y los datos confidenciales.

ID de control	Regla de AWS Config	Directrices
2.3	lambda-inside-vpc	Implemente funciones de AWS Lambda en una Amazon Virtual Private Cloud (Amazon VPC) para obtener una comunicación segura entre una función y otros servicios de Amazon VPC. Con esta configuración, no se requiere ninguna puerta de enlace de internet, dispositivo NAT ni conexión de VPN. Todo el tráfico permanece seguro dentro de la nube de AWS. Debido a su aislamiento lógico, los dominios que residen dentro de una Amazon VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos. Para gestionar correctam ente el acceso, las funciones de AWS Lambda deben asignarse a una VPC.

ID de control	Regla de AWS Config	Directrices
2.3	kms-cmk-not-scheduled-for-deletion	Para ayudar a proteger los datos en reposo, asegúrese de que las claves maestras del cliente (CMK) necesarias no estén programadas para borrado en AWS Key Management Service (AWS KMS). Puesto que a veces es necesario eliminar las claves, esta regla ayuda a comprobar todas las claves cuyo borrado está programado para comprobar si alguna está ahí por error.
2.3	s3-bucket-versioning-enabled	El control de versiones de buckets de Amazon Simple Storage Service (Amazon S3) permite usar múltiples variantes de un objeto en el mismo bucket de Amazon S3. Use el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. El control de versiones ayuda a recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación.

ID de control	Regla de AWS Config	Directrices
2.3	secretsmanager-secret-unused	Si existen credenciales no utilizadas en AWS Secrets Manager, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla le permite establecer un valor en unusedForDays (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.
2.5A	ebs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus volúmenes de Amazon Elastic Block Store (Amazon EBS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.

ID de control	Regla de AWS Config	Directrices
2.5A	ec2-ebs-encryption-by-default	Para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Puesto que puede haber datos confidenc iales en reposo en estos volúmenes, habilite el cifrado en reposo para ayudar a protegerlos.
2.5A	efs-encrypted-check	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de Amazon Elastic File System (EFS).

ID de control	Regla de AWS Config	Directrices
2.5A	efs-in-backup-plan	Para facilitar los procesos de copia de seguridad de datos, asegúrese de que sus sistemas de archivos de Amazon Elastic File System (Amazon EFS) formen parte de un plan de AWS Backup. AWS Backup es un servicio de copia de seguridad totalmente administrado con una solución de copia de seguridad basada en políticas. Esta solución simplifica la administración de copias de seguridad y le permite cumplir con sus requisitos empresariales y normativos de conformidad con las normas de copia de seguridad.
2.5A	encrypted-volumes	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS).
2.5A	kinesis-stream-encrypted	Puesto que puede haber datos confidenciales, para proteger los datos en reposo, asegúrese de habilitar el cifrado para Amazon Kinesis Streams.

ID de control	Regla de AWS Config	Directrices
2.5A	s3-bucket-server-side-encryption-enabled	Para ayudar a proteger los datos en reposo, asegúrese de habilitar el cifrado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de S3, habilite el cifrado para protegerlos.
2.5A	s3-default-encryption-kms	Asegúrese de tener el cifrado habilitado para los buckets de Amazon Simple Storage Service (Amazon S3). Puesto que puede haber datos confidenciales en reposo en los buckets de Amazon S3, habilite el cifrado en reposo para protegerlos.
2.5A	sns-encrypted-kms	Para ayudar a proteger los datos en reposo, asegúrese de que los temas de Amazon Simple Notification Service (Amazon SNS) requieran el cifrado mediante AWS Key Management Service (AWS KMS). Puesto que puede haber datos confidenciales en reposo en los mensajes publicados, habilite el cifrado en reposo para ayudar a protegerlos.

ID de control	Regla de AWS Config	Directrices
4.1	iam-password-policy	Las identidades y las credenciales se emiten, administran y verifican en función de la política de contraseñas de IAM de la organización. Cumplen o superan los requisitos definidos en NIST SP 800-63 y en el estándar Prácticas recomendadas de seguridad básica de AWS para la seguridad de las contraseñas. Esta regla le permite definir de forma opcional RequireUppercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireLowercaseCharacters (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireSymbols (valor de Prácticas recomendadas de seguridad básica de AWS: true), RequireNumbers (valor de Prácticas recomendadas de seguridad básica de AWS: true), MinimumPasswordLength (valor de Prácticas recomendadas de seguridad básica de AWS: 14), PasswordReusePrevention (valor de Prácticas recomendadas de

ID de control	Regla de AWS Config	Directrices
		seguridad básica de AWS: 24) y MaxPasswordAge (valor de Prácticas recomendadas de seguridad básica de AWS: 90) para su política de contraseñ as de IAM. Los valores reales deben reflejar las políticas de su organización.
4.1	access-keys-rotated	Se auditan las credenciales de los dispositivos, usuarios y procesos autorizados para garantizar que las claves de acceso de IAM se roten según la política de la organizac ión. Cambiar las claves de acceso de forma habitual es una práctica recomendada de seguridad. Al hacerlo, se reduce el período de tiempo en el que una clave de acceso está activa y el impacto sobre la empresa si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
4.2	iam-user-mfa-enabled	Active esta regla para restringir el acceso a los recursos en la nube de AWS. Esta regla garantiza que la autenticación multifactor (MFA) esté habilitada para todos los usuarios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Reduzca los incidentes de cuentas comprometidas exigiendo la MFA a los usuarios.
4.2	mfa-enabled-for-iam-console-access	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para todos los usuarios de AWS Identity and Access Management (IAM) que tengan una contraseña de consola. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para los usuarios, puede reducir los incidentes de cuentas comprometidas y evitar que usuarios no autorizados accedan a los datos confidenciales.

ID de control	Regla de AWS Config	Directrices
4.2	root-account-hardware-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA del hardware esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.
4.2	root-account-mfa-enabled	Gestione el acceso a los recursos en la nube de AWS de manera que garantice que la MFA esté habilitada para el usuario raíz. El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La MFA agrega una capa adicional de protección a las credenciales de inicio de sesión. Al requerir la MFA para el usuario raíz, puede reducir los incidente s de las Cuentas de AWS comprometidas.

ID de control	Regla de AWS Config	Directrices
5.1	ec2-instance-profile-attached	Los perfiles de instancia s de EC2 pasan un rol de IAM a una instancia de EC2. Adjuntar un perfil de instancia a las instancias puede ayudar a gestionar los privilegios mínimos y los permisos.
5.1	iam-policy-no-statements-with-full-access	Asegúrese de que las acciones de IAM se limiten únicamente a las acciones necesarias. Permitir que los usuarios tengan más privilegi os de los necesarios para completar una tarea puede infringir el principio de privilegi o mínimo y la separación de funciones.
5.1	iam-root-access-key-check	El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su rol de AWS Identity and Access Management (IAM). Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice cuentas de Cuentas de AWS basadas en roles para ayudar a incorpora r el principio de funcionalidad mínima.

ID de control	Regla de AWS Config	Directrices
5.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) puede ayudarle a restringir los permisos y autorizaciones de acceso al garantizar que los usuarios sean miembros de al menos un grupo. Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea puede infringir el principio de privilegio mínimo y la separación de funciones.
5.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) puede ayudar con los permisos y autorizaciones de acceso al comprobar las contraseñas y claves de acceso de IAM que no se utilicen durante un período de tiempo específico. Si se identifican credenciales no utilizadas, debe deshabilitarlas o eliminarlas, ya que pueden infringir el principio de privilegio mínimo. Esta regla requiere definir un valor para maxCredentialUsageAge (valor predeterminado de Config: 90). El valor real debe reflejar las políticas de su organización.

ID de control	Regla de AWS Config	Directrices
5.4	secretsmanager-rotation-enabled-check	Esta regla garantiza que los secretos de AWS Secrets Manager tengan habilitada la rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela.
5.4	secretsmanager-scheduled-rotation-success-check	Esta regla garantiza que los secretos de AWS Secrets Manager se distribuyan correctamente de acuerdo con el programa de rotación. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si se desvela.
5.4	secretsmanager-secret-periodic-rotation	Esta regla garantiza que los secretos de AWS Secrets Manager tengan habilitad a la rotación periódica. La rotación de los secretos de forma habitual puede acortar el período de vigencia de un secreto y, potencialmente, reducir el impacto sobre la empresa si el secreto se desvela. El valor predeterm inado es 90 días.

ID de control	Regla de AWS Config	Directrices
5.4	secretsmanager-using-cmk	Para ayudar a proteger los datos en reposo, asegúrese de que el cifrado con AWS Key Management Service (AWS KMS) esté habilitado para los secretos de AWS Secrets Manager. Puesto que puede haber datos confidenciales en reposo en secretos de Secrets Manager, habilite el cifrado en reposo para ayudar a protegerlos.
6.4	ec2-instance-detailed-monitoring-enabled	Habilite esta regla para ayudar a mejorar el monitoreo de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la consola de Amazon EC2, que muestra gráficos de monitoreo de la instancia en periodos de 1 minuto.
6.4	cloudwatch-log-group-encrypted	Para ayudar a proteger los datos en reposo confidenciales, asegúrese de que el cifrado esté habilitado para sus grupos de registros de Amazon CloudWatch.

ID de control	Regla de AWS Config	Directrices
6.4	cloud-trail-cloud-watch-logs-enabled	Utilice Amazon CloudWatch para recopilar y administrar de forma centralizada la actividad de los eventos de registro. La inclusión de datos de AWS CloudTrail proporciona detalles de la actividad de llamadas a la API en su Cuenta de AWS.
6.4	cloudtrail-enabled	AWS CloudTrail puede ayudar a evitar el rechazo al registrar las acciones de la Consola de administración de AWS y las llamadas a la API. Puede identificar los usuarios y las Cuentas de AWS que han llamado a un servicio de AWS, la dirección IP de origen desde donde se han generado las llamadas y las horas de las llamadas. Los detalles de los datos capturados se muestran en el contenido de los registros de AWS CloudTrail.
6.4	cloud-trail-encryption-enabled	Dado que pueden existir datos confidenciales, para ayudar a proteger los datos en reposo, debe asegurarse de que el cifrado esté habilitado para sus registros de seguimiento de AWS CloudTrail.

ID de control	Regla de AWS Config	Directrices
6.4	cloud-trail-log-file-validation-enabled	Utilice la validación de los archivos de registro de AWS CloudTrail para comprobar la integridad de los registros de CloudTrail. La validació n de archivos de registro ayuda a determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. Esta caracterí stica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsifica r archivos de registros de CloudTrail sin que se sepa.
6.4	ec2-stopped-instance	Habilite esta regla para facilitar la configuración de referencia de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) al comprobar si las instancia s de Amazon EC2 se han detenido durante más días de los permitidos, de acuerdo con los estándares de su organización.

ID de control	Regla de AWS Config	Directrices
6.4	vpc-flow-logs-enabled	Los registros del flujo de la VPC proporcionan registros detallados acerca del tráfico IP entrante y saliente de las interfaces de red en su Amazon Virtual Private Cloud (Amazon VPC). De forma predeterminada, el registro de flujo incluye valores para los distintos componentes del flujo de IP, incluido el origen, el destino y el protocolo.
6.5A	guardduty-enabled-centralized	Amazon GuardDuty puede ayudar a monitorear y detectar posibles eventos de ciberseguridad mediante fuentes de información sobre amenazas. Estas incluyen listas de IP malintencionadas y machine learning para identificar la actividad inesperada y no permitida, así como la actividad malintencionada en el entorno de la nube de AWS.

ID de control	Regla de AWS Config	Directrices
6.5A	securityhub-enabled	AWS Security Hub ayuda a monitorear el personal, las conexiones, los dispositivos y el software no autorizados. AWS Security Hub agrega, organiza y prioriza las alertas de seguridad o los resultado s de varios servicios de AWS. Algunos de estos servicios son Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Firewall Manager y soluciones de socios de AWS.

Plantilla

La plantilla está disponible en GitHub: Operational Best Practices for SWIFT CSP.

Prácticas de seguridad recomendadas para Amazon Elastic Container Service (Amazon ECS)

Este paquete de conformidad contiene AWS Config reglas basadas en Amazon ECS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub Security Best Practices for Amazon ECS.

Prácticas de seguridad recomendadas para Amazon Elastic File System (Amazon EFS)

Este paquete de conformidad contiene AWS Config reglas basadas en Amazon EFS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub Security Best Practices for Amazon EFS.

Prácticas de seguridad recomendadas para Amazon Elastic Kubernetes Service (Amazon EKS)

Este paquete de conformidad contiene AWS Config normas basadas en Amazon EKS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub Security Best Practices for Amazon EKS.

Mejores prácticas de seguridad para Amazon CloudFront

Este paquete de conformidad contiene AWS Config normas basadas en Amazon CloudFront. Para ver una lista de todas las reglas gestionadas compatibles AWS Config, consulta la Lista de reglas AWS Config gestionadas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Security Best Practices for Amazon CloudFront.

Mejores prácticas de seguridad para Amazon OpenSearch Service

Este paquete de conformidad contiene AWS Config reglas basadas en Amazon OpenSearch Service. Para ver una lista de todas las reglas gestionadas compatibles AWS Config, consulta la Lista de reglas AWS Config gestionadas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Security Best Practices for Amazon OpenSearch Service.

Prácticas de seguridad recomendadas para Amazon Redshift

Este paquete de conformidad contiene AWS Config reglas basadas en Amazon Redshift. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Prácticas recomendadas de seguridad para Amazon Redshift.

Prácticas de seguridad recomendadas para Amazon Relational Database Service (Amazon RDS)

Este paquete de conformidad contiene AWS Config reglas basadas en Amazon RDS. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub Security Best Practices for Amazon RDS.

Mejores prácticas de seguridad para AWS Auto Scaling

Este paquete de conformidad contiene AWS Config reglas basadas en AWS Auto Scaling. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Prácticas recomendadas de seguridad para AWS Auto Scaling.

Mejores prácticas de seguridad para AWS CloudTrail

Este paquete de conformidad contiene AWS Config reglas basadas en AWS CloudTrail. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Prácticas recomendadas de seguridad para AWS CloudTrail.

Mejores prácticas de seguridad para AWS CodeBuild

Este paquete de conformidad contiene AWS Config reglas basadas en AWS CodeBuild. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Prácticas recomendadas de seguridad para AWS CodeBuild.

Prácticas recomendadas de seguridad para Amazon ECR

Este paquete de conformidad contiene reglas de AWS Config basadas en Amazon Elastic Container Registry (Amazon ECR). Para ver una lista de las reglas administradas por AWS Config, consulte List of AWS Config Managed Rules.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Security Best Practices for Amazon ECR.

Mejores prácticas de seguridad para AWS Lambda

Este paquete de conformidad contiene AWS Config reglas basadas en AWS Lambda. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Prácticas recomendadas de seguridad para AWS Lambda.

Mejores prácticas de seguridad para AWS Network Firewall

Este paquete de conformidad contiene AWS Config reglas basadas en AWS Network Firewall. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Prácticas recomendadas de seguridad para AWS Network Firewall.

Prácticas de seguridad recomendadas para Amazon SageMaker AI

Este paquete de conformidad contiene reglas de AWS Config basadas en Amazon SageMaker AI. Para ver una lista de las reglas administradas por AWS Config, consulte List of AWS Config Managed Rules.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Security Best Practices for Amazon SageMaker AI.

Mejores prácticas de seguridad para AWS Secrets Manager

Este paquete de conformidad contiene AWS Config reglas basadas en AWS Secrets Manager. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Prácticas recomendadas de seguridad para AWS Secrets Manager.

Mejores prácticas de seguridad para AWS WAF

Este paquete de conformidad contiene AWS Config reglas basadas en AWS WAF. Para obtener una lista de todas las reglas administradas compatibles AWS Config, consulte la Lista de reglas AWS Config administradas.

Consulte la sección `Parameters` de la siguiente plantilla para ver los nombres y las descripciones de los parámetros obligatorios.

La plantilla está disponible en GitHub: Prácticas recomendadas de seguridad para AWS WAF.

Plantillas de ejemplo con acción de corrección

Prácticas operativas recomendadas para Amazon DynamoDB con corrección

La plantilla está disponible en GitHub Operational Best Practices for Amazon DynamoDB with Remediation.

Prácticas operativas recomendadas para Amazon S3 con corrección

La plantilla está disponible en GitHub: Operational Best Practices for Amazon S3 with Remediation.

Para obtener más información sobre la estructura de las plantillas, consulte Anatomía de la plantilla en la Guía del usuario de AWS CloudFormation.

Creación de plantillas para paquetes de conformidad personalizados para AWS Config

Un paquete de conformidad personalizado es un conjunto único de reglas de AWS Config y acciones de corrección que se puede implementar fácilmente en una cuenta y una región de AWS o en una organización en AWS Organizations.

Para crear un paquete de conformidad personalizado, siga los pasos de la siguiente sección Personalización de la plantilla para crear un archivo YAML que incluya la lista de reglas de AWS Config administradas o las reglas personalizadas de AWS Config con las que quiere trabajar.

Temas

- Terminología
- Personalización de la plantilla

Terminología

Las reglas administradas de AWS Config son reglas predefinidas propiedad de AWS Config.

Las reglas personalizadas de AWS Config son reglas que se crean desde cero.

Hay dos formas de crear reglas personalizadas de AWS Config: con las funciones de Lambda (Guía para desarrolladores de AWS Lambda) y con Guard (Guard GitHub Repository), un lenguaje de políticas como código. Las reglas personalizadas de AWS Config creadas con AWS Lambda se denominan reglas de Lambda personalizadas de AWS Config y las reglas personalizadas de AWS Config creadas con Guard se denominan reglas de políticas personalizadas de AWS Config.

Personalización de la plantilla

Crear el archivo YAML

Para crear un archivo YAML, abra un editor de texto y guarde el archivo como .yaml.

> **Note**
>
> El archivo incluirá una sección Parámetros y una Recursos.

Parámetros

La sección `Parameters` del archivo YAML corresponde a los parámetros de regla del conjunto de reglas de AWS Config que añadirá más adelante en la sección `Resources`. Cree la sección `Parameters` copiando y pegando el siguiente bloque de código en su archivo YAML, personalizándolo según sea necesario y repitiéndolo para cada parámetro de la regla.

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

Por ejemplo:

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> Al seleccionar las reglas de AWS Config para crear el paquete de conformidad personalizado, compruebe que tiene los recursos aprovisionados en su cuenta y que se evaluarán en función de las reglas de AWS Config.

1. La primera línea de la sección de parámetros después de `Parameters:` es una cadena concatenada *`NameOfRule`* + Param + *`NameOfRuleParameter`*.
   a. Sustituya *`NameOfRule`* por un nombre coherente que haya creado para la regla. Por ejemplo, podría ser IamPasswordPolicy para la regla iam-password-policy.
   b. Tipo `Param`.
   c. A continuación, sustituya *`NameOfRuleParameter`* por el nombre del parámetro de la regla especificada. En el caso de las reglas de AWS Config administradas, el nombre del parámetro de regla está en la lista de reglas de AWS Config administradas (por ejemplo, MinimumPasswordLength es el nombre de un parámetro de regla para la regla iam-password-policy). En el caso de las reglas personalizadas de AWS Config, el nombre del parámetro de regla es el nombre elegido al crear la regla.
2. Si utiliza una regla administrada de AWS Config, busque la regla de AWS Config adecuada en la lista de reglas administradas para conocer los valores aceptados para `Default` y `Type` para su regla en particular. En el caso de las reglas personalizadas de AWS Config, utilice los valores seleccionados al crear la regla.

   > **Note**
   >
   > Para cada parámetro debe especificar `Type`. `Type` puede ser String, int, double, CSV, boolean y StringMap.

Recursos

En la sección `Resources` se enumeran las reglas que se van a añadir al paquete de conformidad personalizado. Añada el siguiente bloque `Resources` directamente debajo de la sección `Parameters`, personalícelo según sea necesario y repítalo para cada regla. Para obtener más información sobre las especificaciones, consulte AWS::Config::ConfigRule.

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: !Ref NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
        Type: AWS::Config::ConfigRule
     ...
```

Por ejemplo:

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> Al seleccionar las reglas de AWS Config para crear el paquete de conformidad personalizado, compruebe que dispone de los recursos que se evaluarán para las reglas de AWS Config aprovisionadas en su cuenta. Para obtener más información, consulte Tipos de recursos admitidos.

1. Sustituya *NameOfRule* por el mismo nombre creado en la sección `Parameters`.
2. En el caso de las reglas administradas de AWS Config, sustituya *ActualConfigRuleName* por el título de la página de reglas correspondiente en la Lista de reglas administradas de AWS Config. Para las reglas personalizadas de AWS Config, use el nombre de la regla de Config elegido al crear la regla.

3. Sustituya *NameOfRuleParameter* por el mismo nombre usado en la sección `Parameters`. Después de los dos puntos, copie y pegue la misma cadena concatenada de `!Ref` + *NameOfRule* + Param + *NameOfRuleParameter* que creó en la sección `Parameters`.
4. Cambie *Owner* por el valor adecuado.

> **Note**
>
> Reglas de AWS Config administradas
> En el caso de las reglas de AWS Config administradas, el valor de `Owner` será `AWS`.
> Reglas personalizadas de AWS Config
> En el caso de las reglas personalizadas de AWS Config creadas con Guard, el valor de `Owner` será `CUSTOM_POLICY`. En el caso de las reglas personalizadas de AWS Config creadas con Lambda, el valor de `Owner` será `CUSTOM_LAMBDA`.

5. Cambie *SOURCE_IDENTIFIER* por el valor adecuado.

> **Note**
>
> Reglas de AWS Config administradas
> En el caso de las reglas de AWS Config administradas, copie el identificador siguiendo el enlace de la regla que seleccione en la Lista de reglas de AWS Config administradas (por ejemplo, el identificador de origen de la regla access-keys-rotated es ACCESS_KEYS_ROTATED).
> Reglas personalizadas de AWS Config
> Para las reglas personalizadas de AWS Config creadas con Lambda, el `SourceIdentifier` es el nombre de recurso de Amazon (ARN) de la función de AWS Lambda de la regla, como `arn:aws:lambda:us-east-2:123456789012:function:`*ActualConfigRuleName*. Para las reglas personalizadas de AWS Config creadas con Guard, este campo no es necesario.

En conjunto, el paquete de conformidad personalizado que ha rellenado debería empezar a tener un aspecto similar al siguiente, que es un ejemplo en el que se utilizan estas reglas de AWS Config administradas: iam-password-policy, access-keys-rotated e iam-user-unused-credentials-check

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
```

```
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: !Ref AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge: !Ref
 IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

Implementación de paquetes de conformidad para AWS Config

Puede utilizar la consola de AWS Config o la AWS CLI para implementar paquetes de conformidad.

Deploy Conformance Packs (Console)

En la página Conformance packs (Paquetes de conformidad), puede implementar un paquete de conformidad de una cuenta en una región. También puede editar y eliminar el paquete de conformidad implementado.

Puede implementar un paquete de conformidad mediante plantillas de ejemplo de AWS Config o su propia plantilla personalizada. Para obtener instrucciones sobre cómo crear paquetes de conformidad personalizados, consulte Paquete de conformidad personalizado.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Config en https://console.aws.amazon.com/config/home.
2. Acceda a la página Conformance packs (Paquetes de conformidad)y seleccione Deploy conformance pack (Implementar paquete de conformidad).
3. En la página Specify template (Especifique una plantilla), seleccione una plantilla de ejemplo o una plantilla existente. Para obtener más información, consulte Plantillas de ejemplo del paquete de conformidad.

   - Si elige Utilizar una plantilla de muestra, seleccione una plantilla de muestra en la lista desplegable.

     Para obtener más información sobre el contenido de cada plantilla, consulte Plantillas de ejemplo del paquete de conformidad.
   - Si elige Template is ready (La plantilla está lista), especifique el origen de la plantilla. Puede ser un URI de Amazon S3, un documento de AWS Systems Manager (documento SSM) o una plantilla que cargue.

     Si la plantilla tiene más de 50 kB, cárguela en el bucket de S3 y seleccione esa ubicación. Por ejemplo: s3://*nombrdelbucket/prefijo*.

     > **Important**
     >
     > Elija La plantilla está lista si ha creado el archivo YAML del paquete de conformidad desde cero basándose en el paquete de conformidad personalizado.

4. Elija Siguiente.
5. En la página Especificar los detalles del paquete de conformidad, escriba el nombre del paquete de conformidad.

El nombre del paquete de conformidad debe ser único y tener un máximo de 256 caracteres alfanuméricos. El nombre puede contener guiones, pero no espacios.

6. Opcional: añada un parámetro.

   Los parámetros se definen en la plantilla y le ayudan a administrar y organizar los recursos.

7. Elija Siguiente.
8. En la página Review and deploy (Revisar e implementar), revise toda la información.

   Puede editar los detalles de la plantilla y los detalles del paquete de conformidad utilizando Edit (Editar).

9. Seleccione Deploy conformance pack (Implementar paquete de conformidad).

   AWS Config muestra el paquete de conformidad en la página correspondiente con el estado adecuado.

   Si se produce un error en la implementación del paquete de conformidad, compruebe los permisos y los requisitos previos e inténtelo de nuevo. Puede ponerse en contacto con AWS Support.

Para implementar un paquete de conformidad utilizando una plantilla de ejemplo con correcciones, consulte A. Requisitos previos para utilizar un paquete de conformidad con corrección y el procedimiento anterior.

Para implementar un paquete de conformidad con una o varias reglas de AWS Config, consulte B. Requisitos previos para utilizar un paquete de conformidad con una o más reglas personalizadas AWS Config.

Deploy Conformance Packs (AWS CLI)

1. Abra un símbolo del sistema o una ventana de terminal.
2. Introduzca uno de los siguientes comandos para implementar un paquete de conformidad llamado **`MyConformancePack`**. El origen de la plantilla puede ser un URI de Amazon S3, una plantilla que cargue o un documento de AWS Systems Manager (documento SSM).

   URI de Amazon S

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   ```

```
--template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
--delivery-s3-bucket amzn-s3-demo-bucket
```

Plantilla YAML de su directorio local

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-body template body
```

AWS Systems Manager Documento (documento de Systems Manager)

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-ssm-document-details
 DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
--delivery-s3-bucket amzn-s3-demo-bucket
```

3. Pulse Intro para ejecutar el comando.

   Debería ver un resultado similar a este.

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> Para obtener más información sobre cómo crear una plantilla YAML para un paquete de conformidad, consulte Paquete de conformidad personalizado.

Edición de paquetes de conformidad para AWS Config

Puede utilizar la consola de AWS Config o la AWS CLI para editar paquetes de conformidad.

Editing Conformance Packs (Console)

1. Para editar un paquete de conformidad, selecciónelo en la tabla.

2. Elija Acciones y, a continuación, elija Editar.
3. En la página Edit conformance pack (Editar paquete de conformidad), puede editar los detalles de la plantilla, el paquete de conformidad y la sección de parámetros.

   No puede cambiar el nombre del paquete de conformidad.
4. Seleccione Save changes (Guardar cambios).

   El paquete de conformidad aparece con las reglas de AWS Config.

Editing Conformance Packs (AWS CLI)

Si está editando un paquete de conformidad que ha añadido anteriormente, utilice el mismo comando `PutConformancePack` que utilizó al implementar un paquete de conformidad.

1. Abra un símbolo del sistema o una ventana de terminal.
2. Introduzca uno de los siguientes comandos para implementar un paquete de conformidad llamado **`MyConformancePack`**. El origen de la plantilla puede ser un URI de Amazon S3, una plantilla que cargue o un documento de AWS Systems Manager (documento SSM).

   URI de Amazon S

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

   Plantilla YAML de su directorio local

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   AWS Systems Manager Documento (documento de Systems Manager)

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-ssm-document-details
    DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

3. Pulse Intro para ejecutar el comando.

   Debería ver un resultado similar a este.

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> Para obtener más información sobre cómo crear una plantilla YAML para un paquete de conformidad, consulte Paquete de conformidad personalizado.

Eliminación de paquetes de conformidad para AWS Config

Puede utilizar la consola de AWS Config o la AWS CLI para eliminar paquetes de conformidad.

Consideraciones

Recomendación: considere excluir el tipo de recurso **`AWS::Config::ResourceCompliance`** del registro antes de eliminar reglas

Al eliminar las reglas, se crean elementos de configuración (CI) para `AWS::Config::ResourceCompliance`, lo que puede afectar a los costos del registrador de configuración. Si elimina reglas que evalúan una gran cantidad de tipos de recursos, esto puede provocar un aumento en el número de elementos de configuración registrados.

Para evitar los costos asociados, puede optar por deshabilitar el registro para el tipo de recurso `AWS::Config::ResourceCompliance` antes de eliminar reglas y volver a habilitarlo una vez eliminadas las reglas.

Sin embargo, dado que la eliminación de reglas es un proceso asincrónico, puede tardar una hora o más en completarse. Durante el tiempo en que el registro esté deshabilitado para `AWS::Config::ResourceCompliance`, las evaluaciones de reglas no se registrarán en el historial de recursos asociado.

Cómo eliminar un paquete de conformidad

Deleting Conformance Packs (Console)

1. Para suprimir un paquete de conformidad, selecciónelo en la tabla.
2. Elija Acciones y, a continuación, elija Eliminar.
3. En el cuadro de diálogo *Delete conformance pack (Suprimir paquete de conformidad)*, confirme si desea eliminar permanentemente este paquete de conformidad.

   > **Important**
   >
   > Esta acción no se puede revertir. Si elimina un paquete de conformidad, se suprimirán todas las reglas y acciones de corrección de AWS Config de dicho paquete.

4. Escriba Delete (Suprimir) y haga clic en Delete (Suprimir).

   En la página Conformance packs (Paquetes de conformidad), aparecerá el estado de implementación Deleting (Eliminando) hasta que se elimine completamente el paquete de conformidad.

Deleting Conformance Packs (AWS CLI)

Escriba el siguiente comando.

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

Si se ejecuta correctamente, el comando no muestra ninguna otra salida.

> **Important**
>
> Esta acción no se puede revertir. Si elimina un paquete de conformidad, se suprimirán todas las reglas y acciones de corrección de AWS Config de dicho paquete.

Visualización de detalles e información de conformidad en los paquetes de conformidad para AWS Config

> **Important**
>
> Para obtener informes precisos sobre el estado de cumplimiento, debe registrar el tipo de recurso de `AWS::Config::ResourceCompliance`. Para obtener más información, consulte Recording AWS Resources.

Puede utilizar la consola de AWS Config o la AWS CLI para ver los paquetes de conformidad. La consola de AWS Config tiene un panel de control unificado. La AWS CLI le permite ejecutar comandos para obtener información específica.

Viewing Conformance Packs (Console)

Para ver los paquetes de conformidad en la Consola de administración de AWS, consulte Conformance Pack Dashboard Pack.

Viewing the Details for your Conformance Packs (AWS CLI)

1. Escriba el siguiente comando.

```
aws configservice describe-conformance-packs
```

O BIEN

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. Debería ver un resultado similar a este.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

Viewing the Status for your Conformance Packs (AWS CLI)

1. Escriba el siguiente comando.

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. Debería ver un resultado similar a este.

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

Viewing the Compliance Status for your Conformance Packs (AWS CLI)

1. Escriba el siguiente comando.

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. Debería ver un resultado similar a este.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
```

```
        }
    ]
}
```

Viewing the Compliance Details for your Conformance Packs (AWS CLI)

1. Escriba el siguiente comando.

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. Debería ver un resultado similar a este.

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
```

```
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

Visualización del cronograma del historial de cumplimiento de los paquetes de conformidad para AWS Config

AWS Config permite almacenar los cambios de estado de conformidad en sus paquetes de conformidad. De este modo, puede ver el historial de cambios del estado de conformidad. Estos cambios del estado de conformidad se presentan como una línea de tiempo. La línea de tiempo captura los cambios como `ConfigurationItems` a lo largo de un periodo de tiempo. También puede utilizar esta característica para buscar reglas específicas que no sean conformes dentro de un paquete de conformidad.

Puede optar o no por registrar todos los tipos de recursos en AWS Config. Si ha optado por registrar todos los tipos de recursos, comienza a registrar AWS Config automáticamente el historial de conformidad del paquete de conformidad según lo evaluado por AWS Config Rules. De forma predeterminada, AWS Config registra los cambios de configuración de todos los recursos compatibles. También puede seleccionar solo el tipo de recurso del historial de conformidad específico del paquete de conformidad: `AWS::Config::ConformancePackCompliance`. El registro del tipo de recurso `AWS::Config::ConformancePackCompliance` no tiene costo adicional. Para obtener más información, consulte AWS Recursos de grabación.

Un paquete de conformidad es conforme si todas las reglas de un paquete de conformidad lo son. No es conforme si alguna de las reglas no lo es. El estado de conformidad de un paquete de conformidad es INSUFFICIENT_DATA solo si no se pueden evaluar todas las reglas de un paquete de conformidad por falta de datos. Si algunas de las reglas de un paquete de conformidad son conformes, pero el estado de conformidad de otras reglas del mismo paquete de conformidad es INSUFFICIENT_DATA, el paquete de conformidad indica que son conformes. El cumplimiento de un paquete de conformidad no se evalúa de una sola vez. Es posible que la evaluación de algunas reglas lleve más tiempo que otras. La conformidad se evalúa por grupos de reglas de forma simultánea y continúa por etapas hasta que se hayan evaluado todas las reglas de un paquete de conformidad.

Visualización de la línea de tiempo de conformidad

Para acceder a la línea de tiempo de conformidad, seleccione un paquete de conformidad específico en la página principal del paquete de conformidad.

1. Navegue a la página Paquete de conformidad.
2. En la página principal de Paquete de conformidad, elija un paquete de conformidad específico y, a continuación, Línea de tiempo del paquete de conformidad.

> **Note**
>
> Como alternativa, puede utilizar la línea de tiempo de conformidad de la página de detalles del paquete de conformidad. Elija un paquete de conformidad y Ver detalles en el menú desplegable Acciones. En esta página, elija Línea de tiempo del paquete de conformidad.

La línea de tiempo muestra el historial de cambios del estado de conformidad de un paquete de conformidad. Se puede hacer lo siguiente:

1. Amplíe un cambio de conformidad para ver el estado de line-by-line conformidad de cada regla de un paquete de conformidad.
2. En la vista expandida, elija una regla específica para ver su página de detalles.

Consulta del historial de conformidad de los paquetes de conformidad para AWS Config

Consulte el historial de conformidad get-resource-config-history utilizando el tipo de recurso. `AWS::Config::ConformancePackCompliance`

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

Debería ver una salida similar a esta:

```
{
    "configurationItems": [
        {
            "version": "1.3",
```

```
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
```

```
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

Para obtener más información, consulta los tipos de recursos admitidos (AWS Config) y GetResourceConfigHistoryla referencia de la API.

Gestión de paquetes de conformidad para AWS Config todas las cuentas de su organización

Se utilizan AWS Config para gestionar los paquetes de conformidad Cuentas de AWS en todos los componentes de una organización. Se puede hacer lo siguiente:

- Implemente, actualice y elimine paquetes de conformidad en las cuentas miembro de una organización de AWS Organizations.
- Implemente un conjunto común de AWS Config reglas y acciones correctivas en todas las cuentas y especifique las cuentas en las que no se deben crear AWS Config reglas y acciones correctivas.
- Utilice la cuenta de administración AWS Organizations para reforzar la gobernanza, asegurándose de que las cuentas de los miembros de su organización no puedan modificar las AWS Config reglas subyacentes y las medidas correctivas.

Consideraciones

Para implementaciones en diferentes regiones

La llamada a la API para implementar reglas y paquetes de conformidad en todas las cuentas es AWS específica de cada región. En el nivel de organización, debe cambiar el contexto de la llamada a la API a una región diferente si quiere implementar reglas en otras regiones. Por ejemplo, para

implementar una regla en Este de EE. UU. (Norte de Virginia), cambie la región a Este de EE. UU. (Norte de Virginia) y, a continuación, llame a `PutOrganizationConfigRule`.

Para cuentas dentro de una organización

Si una cuenta nueva se une a una organización, la regla o el paquete de conformidad se implementan en esa cuenta. Cuando una cuenta abandona una organización, se elimina la regla o el paquete de conformidad.

Si implementa una regla organizativa o un paquete de conformidad en una cuenta de administrador de la organización y, a continuación, establece un administrador delegado e implementa una regla organizativa o un paquete de conformidad en la cuenta de administrador delegado, no podrá ver la regla organizativa ni el paquete de conformidad en la cuenta de administrador de la organización desde la cuenta de administrador delegado ni ver la regla organizativa ni el paquete de conformidad en la cuenta de administrador delegado desde la cuenta de administrador de la organización. El DescribeOrganizationConfigRulesy solo DescribeOrganizationConformancePacks APIs puede ver e interactuar con los recursos relacionados con la organización que se implementaron desde la cuenta que los llama. APIs

Mecanismo de reintento para las cuentas nuevas que se agreguen a una organización

Si no hay ningún registrador disponible, solo se volverán a intentar implementar las reglas organizativas y los paquetes de conformidad existentes durante 7 horas después de añadir una cuenta a su organización. Se espera que cree un registrador si no existe uno dentro de las 7 horas siguientes a la adición de una cuenta a su organización.

Cuentas de administración de la organización, administradores delegados y roles vinculados a servicios

Si utilizas una cuenta de administración de la organización y piensas usar un administrador delegado para el despliegue organizacional, ten en cuenta que eso AWS Config no creará automáticamente el rol vinculado al servicio (SLR). Debe crear el rol vinculado al servicio (SLR) manualmente y por separado, mediante IAM.

Si no tiene un SLR para la cuenta de administración, no podrá implementar recursos en esa cuenta desde una cuenta de administrador delegado. Podrá seguir implementando paquetes de conformidad en las cuentas de los miembros desde las cuentas de administración y de administrador delegado. Para obtener más información, consulte Uso de roles vinculados a servicios en la Guía del usuario de AWS Identity and Access Management (IAM).

Implementación

To deploy with the Consola de administración de AWS

Para implementar un paquete de conformidad en una organización desde la consola, utilice. AWS AWS Systems Manager Para obtener más información, consulte Implementar paquetes de AWS Config conformidad en la Guía del AWS Systems Manager usuario.

To deploy with the AWS API

Para obtener información sobre cómo realizar la integración AWS Config con AWS Organizations, consulte AWS Config y AWS Organizations en la Guía del AWS Organizations usuario. Asegúrese de que la AWS Config grabación esté activada antes de utilizar lo siguiente APIs para gestionar las reglas del paquete de conformidad Cuentas de AWS en toda la organización:

- DeleteOrganizationConformancePack, elimina el paquete de conformidad de la organización especificado y todas las reglas de configuración y las acciones correctivas de todas las cuentas de los miembros de esa organización.
- DescribeOrganizationConformancePacks, devuelve una lista de los paquetes de conformidad de la organización.
- DescribeOrganizationConformancePackStatuses, proporciona el estado de despliegue del paquete de conformidad organizacional para una organización.
- GetOrganizationConformancePackDetailedStatus, devuelve el estado detallado de cada cuenta de miembro de una organización para un paquete de conformidad de la organización determinado.
- PutOrganizationConformancePack, despliega paquetes de conformidad en las cuentas de los miembros de una organización. AWS

Compatibilidad de la región

En las siguientes regiones se admite la implementación de paquetes de conformidad en las cuentas de los miembros de una AWS organización.

Nombre de la región	Región	Punto de conexión	Protocolo	
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
Este de EE. UU. (Norte de Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
Oeste de EE. UU. (Norte de California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
Asia-Pacífico (Tailandia)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
México (centro)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Solución de problemas en paquetes de conformidad para AWS Config

Compruebe los siguientes elementos para solucionar los problemas que puedan surgir al utilizar los paquetes de conformidad.

Temas

- Estado fallido de un paquete de conformidad
- Reglas colgantes en un paquete de conformidad

Estado fallido de un paquete de conformidad

Si aparece un error que indica que el paquete de conformidad no se pudo crear, actualizar o eliminar correctamente, puede comprobar el estado del paquete de conformidad.

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

Debería ver un resultado similar a este.

```
"ConformancePackStatusDetails": [
```

```
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

Consulte ConformancePackStatusReason para obtener más información sobre el error.

Cuando el valor de stackArn está presente en la respuesta

Si el mensaje de error no está claro o si el error es interno, vaya a la consola de CloudFormation y haga lo siguiente:

1. Busque el valor de stackArn en la salida.
2. Seleccione la pestaña Eventos de la pila de CloudFormation y consulte los eventos con errores.

   El motivo del estado indica por qué se produjeron errores en el paquete de conformidad.

Cuando el valor de stackArn no está presente en la respuesta

Si recibe un error mientras crea el paquete de conformidad, pero el valor de stackArn no está presente en la respuesta de estado, lo más probable es que el error se produjera al crear la pila y que CloudFormation la haya revertido y eliminado. Vaya a la consola de CloudFormation y busque pilas que tengan el estado Eliminado. Es posible que la pila errónea esté disponible allí. La pila de CloudFormation contiene el nombre del paquete de conformidad. Si encuentra la pila con errores, elija la pestaña Eventos de la pila de CloudFormation y compruebe si hay eventos con errores.

Si ninguno de los pasos anteriores funciona y el motivo es un error de servicio interno, intente repetir la operación o póngase en contacto con el Centro de AWS Support.

Reglas colgantes en un paquete de conformidad

La implementación de un paquete de conformidad implica crear una pila de AWS CloudFormation subyacente en segundo plano para implementar las reglas en la plantilla del paquete de

conformidad. Estas reglas son reglas vinculadas a un servicio y no se pueden actualizar ni eliminar fuera del paquete de conformidad.

Si hace cambios en la pila de CloudFormation subyacente, se produce una situación en la que el paquete de conformidad y sus reglas se vuelven inadministrables. Estas reglas inadministrables se denominan reglas colgantes.

Desviación entre la pila de CloudFormation y el paquete de conformidad

Puede actualizar los nombres de las reglas en una plantilla de paquete de conformidad directamente desde la consola de CloudFormation. Si actualiza la plantilla directamente desde la consola de CloudFormation, el paquete de conformidad implementado no se actualizará.

Esta desviación crea una regla colgante. Si intenta eliminar la regla del paquete de conformidad, recibirá un error similar al siguiente:

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

Si intenta eliminar la regla del paquete de conformidad, la regla colgante no se podrá eliminar y recibirá un error similar al siguiente:

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

Para solucionar este problema, siga estos pasos:

1. Elimine la pila. Para obtener más información, consulte Eliminar una pila de la consola de CloudFormation en la Guía del usuario de CloudFormation.
2. Elimine el paquete de conformidad mediante la consola de AWS Config o mediante la API DeleteConformancePack. Si se trata de un paquete de conformidad organizativo y utiliza la cuenta de administración o de administrador delegado, use la API DeleteOrganizationConformancePack.
3. Póngase en contacto con el Centro de AWS Support, con el nombre de recurso de Amazon (ARN) de las reglas colgantes del paquete de conformidad, a fin de recibir asistencia para limpiar la cuenta.

Para evitar este problema, recuerde estas prácticas recomendadas:

- No actualice nunca directamente la pila de CloudFormation de un paquete de conformidad.
- Nunca intente realizar cambios que generen desviaciones entre el paquete de conformidad y su pila subyacente en CloudFormation.
- El rol vinculado a un servicio (SLR) de los paquetes de conformidad no se puede modificar. Compruebe que los recursos que va a actualizar formen parte de la política de permisos del SLR.

Pila de CloudFormation eliminada para un paquete de conformidad

A menos que haya diferencias entre la pila de CloudFormation y el paquete de conformidad, nunca es recomendable eliminar las reglas de un paquete de conformidad, o de su pila de CloudFormation, directamente desde la consola de CloudFormation.

Para resolver este problema, póngase en contacto con el Centro de AWS Support, con el nombre de recurso de Amazon (ARN) de las reglas colgantes del paquete de conformidad, a fin de recibir asistencia para limpiar la cuenta.

Para evitar este problema, recuerde estas prácticas recomendadas:

- No elimine nunca la pila de CloudFormation subyacente para un paquete de conformidad.
- Elimine los paquetes de conformidad mediante la API DeleteConformancePack. Si se trata de un paquete de conformidad organizativo y utiliza la cuenta de administración o de administrador delegado, use la API DeleteOrganizationConformancePack.

Corregir los recursos no conformes con AWS Config

AWS Config permite corregir los recursos no conformes que son evaluados por. Reglas de AWS Config AWS Config aplica la corrección mediante AWS Systems Manager documentos de automatización. Estos documentos definen las acciones que se deben realizar con los AWS recursos no conformes evaluados por. Reglas de AWS Config Puede asociar documentos SSM utilizando Consola de administración de AWS o utilizando. APIs

AWS Config proporciona un conjunto de documentos de automatización gestionada con acciones correctivas. También puede crear y asociar documentos de automatización personalizados a las AWS Config reglas.

Temas

- Compatibilidad de la región
- Configuración de la remediación manual para AWS Config
- Configuración de la remediación automática para AWS Config
- Eliminar acciones de remediación para AWS Config

Compatibilidad de la región

Actualmente, se admiten acciones correctivas para AWS Config Rules en las siguientes regiones:

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Este de EE. UU. (Norte de Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Oeste de EE. UU. (Norte de California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Configuración de la remediación manual para AWS Config

Para aplicar medidas correctivas a los recursos no conformes, puede elegir la acción correctiva que desee asociar de una lista rellenada previamente o crear sus propias acciones correctivas personalizadas utilizando documentos SSM. AWS Config proporciona una lista recomendada de medidas correctivas en el. Consola de administración de AWS

Setting Up Manual Remediation (Console)

En el Consola de administración de AWS, puede optar por corregir manualmente los recursos no conformes asociando las acciones de corrección a las reglas. AWS Config Con todas las acciones de corrección, puede elegir la corrección manual o automática.

1. Inicie sesión en la consola de su casa Consola de administración de AWS y ábrala. AWS Config https://console.aws.amazon.com/config/
2. Elija Reglas a la izquierda y, a continuación, en la página Reglas, elija Agregar regla para añadir reglas nuevas a la lista de reglas.

Si se trata de una regla existente, seleccione la regla no conforme en la lista y elija la lista desplegable Acciones.

3. En la lista desplegable Acciones, seleccione Administrar corrección. Seleccione Corrección manual y, a continuación, elija la acción de corrección adecuada de la lista recomendada.

> **Note**
>
> Solo puede gestionar las correcciones de las reglas no vinculadas AWS Config a un servicio. Para obtener más información, consulte Service-Linked AWS Rules.

En función de la acción de corrección seleccionada, verá parámetros específicos o no verá ningún parámetro.

4. (Opcional) Si desea pasar el ID de recurso de los recursos no conformes a la acción de corrección, elija Resource ID parameter (Parámetro de ID de recurso). Si se selecciona esta opción, ese parámetro se sustituye por el ID del recurso que se va a corregir en tiempo de ejecución.

   Cada parámetro tiene un valor estático o un valor dinámico. Si no elige un parámetro de ID de recurso específico en la lista desplegable, puede especificar valores para cada clave. Si elige un parámetro de ID de recurso en la lista desplegable, puede especificar valores para todas las demás claves, excepto el parámetro de ID de recurso seleccionado.

5. Seleccione Save. Aparece la página Rules (Reglas).

Para solucionar problemas de las acciones de corrección fallidas, puede ejecutar el AWS comando de la interfaz de línea de comandos `describe-remediation-execution-status` para obtener una vista detallada de la ejecución de una corrección para un conjunto de recursos. Los detalles incluyen el estado, las marcas temporales para los pasos de ejecución de corrección y cualquier mensaje de error que corresponda a los pasos con error.

Setting Up Manual Remediation (API)

Utilice la siguiente operación AWS Config de API para configurar la corrección manual:

- PutRemediationConfigurations, agrega o actualiza la configuración de corrección con una AWS Config regla específica con el objetivo o la acción seleccionados.

- StartRemediationExecution, ejecuta una corrección bajo demanda para las AWS Config reglas especificadas en función de la última configuración de corrección conocida.
- DescribeRemediationExecutionStatus, proporciona una vista detallada de la ejecución de una corrección para un conjunto de recursos, que incluye el estado, las marcas de tiempo en las que se llevan a cabo las medidas de ejecución de la corrección y cualquier mensaje de error de las medidas que hayan fallado.
- DescribeRemediationConfigurations, devuelve los detalles de una o más configuraciones de corrección.

Configuración de la remediación automática para AWS Config

Para aplicar medidas correctivas a los recursos no conformes, puede elegir la acción correctiva que desee asociar de una lista rellenada previamente o crear sus propias acciones correctivas personalizadas utilizando documentos SSM. AWS Config proporciona una lista de las medidas correctivas en el. Consola de administración de AWS

Setting Up Auto Remediation (Console)

En el Consola de administración de AWS, puede optar por corregir automáticamente los recursos no conformes asociando las acciones de corrección a las reglas. AWS Config Con todas las acciones de corrección, puede elegir la corrección manual o automática.

1. Inicie sesión en la consola de su casa Consola de administración de AWS y ábrala. AWS Config https://console.aws.amazon.com/config/
2. Elija Rules (Reglas) a la izquierda y, a continuación, en la página Rules (Reglas), elija Add Rule (Añadir regla) para añadir reglas nuevas a la lista de reglas.

   Si se trata de una regla existente, seleccione la regla no conforme en la lista y elija la lista desplegable Acciones.
3. En la lista desplegable Acciones, seleccione Administrar corrección. Seleccione “Corrección automática” y, a continuación, elija la acción de corrección adecuada de la lista.

> **Note**
>
> Solo puede gestionar las correcciones de las reglas no vinculadas AWS Config a un servicio. Para obtener más información, consulte Service-Linked AWS Rules.

En función de la acción de corrección seleccionada, verá parámetros específicos o no verá ningún parámetro.

4. Elija Auto remediation (Corrección automática) para solucionar automáticamente los recursos no conformes.

   Si un recurso sigue siendo no conforme después de la corrección automática, puede configurar la regla para que intente realizar de nuevo la corrección automática. Escriba los reintentos y segundos deseados.

   > **Note**
   >
   > Existen costos asociados con la ejecución de un script de corrección varias veces. Los reintentos solo se producen si la corrección falla y funcionan dentro del período de tiempo especificado; por ejemplo, 5 reintentos en 300 segundos. Para obtener más información, consulte Precios de automatización de Systems Manager.

5. (Opcional) Si desea pasar el ID de recurso de los recursos no conformes a la acción de corrección, elija Resource ID parameter (Parámetro de ID de recurso). Si se selecciona esta opción, ese parámetro se sustituye por el ID del recurso que se va a corregir en tiempo de ejecución.

   Cada parámetro tiene un valor estático o un valor dinámico. Si no elige un parámetro de ID de recurso específico en la lista desplegable, puede especificar valores para cada clave. Si elige un parámetro de ID de recurso en la lista desplegable, puede especificar valores para todas las demás claves, excepto el parámetro de ID de recurso seleccionado.

6. Seleccione Save. Aparece la página Rules (Reglas).

Resolución de problemas relacionados con las acciones de corrección fallidas

Para solucionar problemas de las acciones de corrección fallidas, puede ejecutar el AWS comando de la interfaz de línea de comandos `describe-remediation-execution-status` para obtener una vista detallada de la ejecución de una corrección para un conjunto de recursos. Los detalles incluyen el estado, las marcas temporales para los pasos de ejecución de corrección y cualquier mensaje de error que corresponda a los pasos con error.

La corrección automática se puede iniciar incluso para recursos conformes

Si habilitas la corrección automática para una AWS Config regla específica mediante la PutRemediationConfigurationsAPI o la AWS Config consola, se inicia el proceso de corrección para todos los recursos que no cumplen con esa regla específica. El proceso de corrección automática se basa en la instantánea de los datos de cumplimiento, que se captura periódicamente. Cualquier recurso no conforme que se actualice entre el programa de instantáneas se seguirá corrigiendo en función de la última instantánea de datos de cumplimiento conocida.

Esto significa que, en algunos casos, se puede iniciar una corrección automática incluso para los recursos que cumplen con las normas, ya que el procesador de arranque utiliza una base de datos que puede tener resultados de evaluación obsoletos, basados en la última instantánea de datos de conformidad conocida.

Setting Up Auto Remediation (API)

Utilice la siguiente operación de AWS Config API para configurar la corrección automática:

- PutRemediationExceptions, agrega una nueva excepción o actualiza una excepción existente para un recurso específico con una AWS Config regla específica.
- DescribeRemediationExceptions, devuelve los detalles de una o más excepciones de corrección.

Eliminar acciones de remediación para AWS Config

Puede utilizar la AWS Config consola o la AWS CLI para eliminar las acciones correctivas.

Deleting remediation actions (Console)

1. Inicie sesión en la AWS Config consola Consola de administración de AWS y ábrala en https://console.aws.amazon.com/config/casa.
2. Seleccione Reglas a la izquierda y, en la página Reglas, seleccione la regla en la lista y elija Editar.
3. En la *name of the rule* página, vaya a la sección Medidas correctivas. Amplíe la sección para ver detalles adicionales.
4. En la sección Acción de corrección, elija Eliminar y confirme la acción de eliminación.

> **Note**
>
> Si la corrección está en curso, la acción de corrección no se eliminará. Si selecciona Eliminar la acción de corrección, no podrá recuperar esta acción. La acción de corrección no elimina la regla asociada.

Si se elimina una acción de corrección, el Parámetro de ID del recurso estará vacío y mostrará N/A. En la página Reglas, la columna de acción de corrección muestra Sin definir para la regla asociada.

Deleting remediation actions (API)

Utilice la siguiente operación de AWS Config API para configurar la corrección automática:

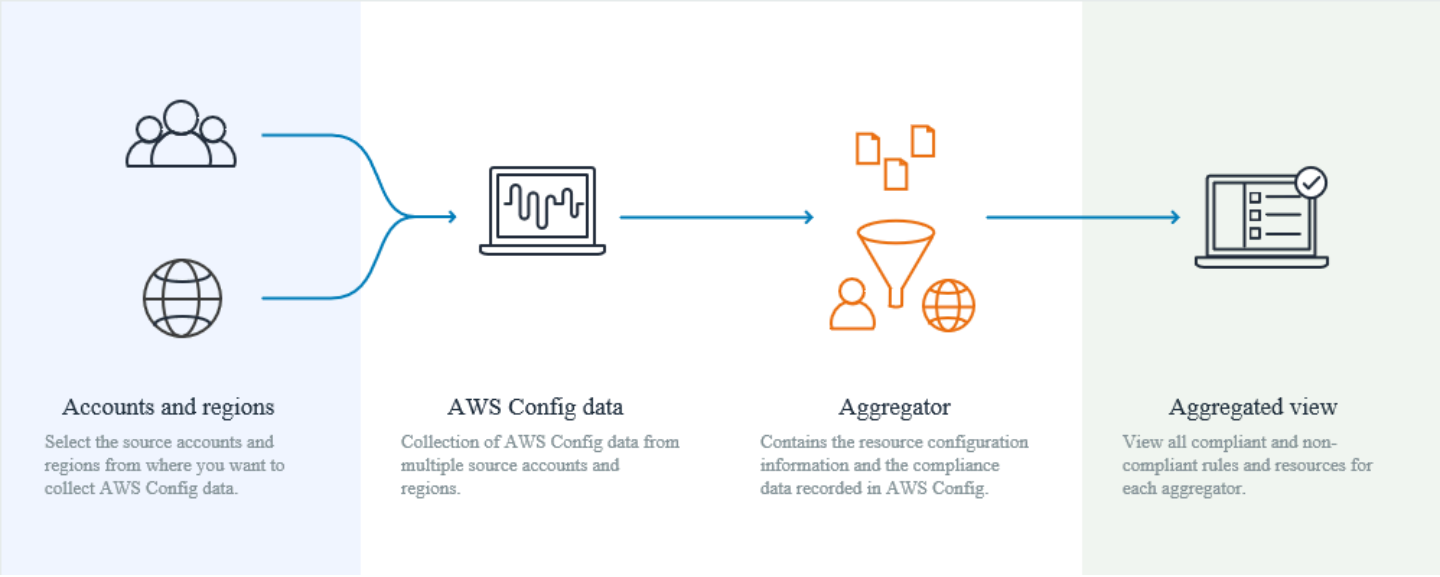
- DeleteRemediationConfiguration, elimina la configuración de corrección.
- DeleteRemediationExceptions, elimina una o más excepciones de corrección mencionadas en las claves de recursos.

Agregación de datos multicuenta y multirregión para AWS Config

Un agregador es un tipo AWS Config de recurso que recopila datos AWS Config de configuración y conformidad de lo siguiente:

- Varias cuentas y varias AWS regiones.
- Cuenta única y varias AWS regiones.
- Una organización AWS Organizations y todas las cuentas de esa organización que AWS Config estén habilitadas.

Utilice un agregador para ver la configuración de recursos y los datos de conformidad registrados en AWS Config. La siguiente imagen muestra cómo un agregador recopila AWS Config datos de varias cuentas y regiones.



Casos de uso

- Supervisión del cumplimiento: puede agregar datos de cumplimiento para evaluar las posturas generales de cumplimiento de su organización o de todas las cuentas y regiones.
- Seguimiento de cambios: puede hacer un seguimiento de los cambios en los recursos a lo largo del tiempo en toda su organización o en todas las cuentas y regiones.

- Relaciones de recursos: puede analizar las dependencias y relaciones de los recursos en toda su organización o en todas las cuentas y regiones.

> **Note**
>
> Los agregadores proporcionan una vista de solo lectura de las cuentas y regiones de origen que el agregador está autorizado a ver; para ello, replican los datos de las cuentas de origen en la cuenta del agregador. Los agregadores no proporcionan acceso mutante ni a la cuenta ni a la región de origen. Por ejemplo, esto significa que no puede implementar reglas a través de un agregador ni enviar archivos de instantáneas a una cuenta o región de origen a través de un agregador.
> El uso de agregadores no implica ningún costo adicional.

Terminología

Una cuenta de origen es la cuenta Cuenta de AWS desde la que desea agregar los datos de conformidad y configuración AWS Config de los recursos. Una cuenta de origen puede ser una cuenta individual o una organización de AWS Organizations. Puede proporcionar las cuentas de origen de forma individual o puede recuperarlas a través de ellas AWS Organizations.

Una región de origen es la AWS región desde la que desea agregar los datos AWS Config de configuración y conformidad.

Una cuenta de agregador es la cuenta en la que se crea un agregador.

La autorización se refiere a los permisos que se conceden a una cuenta y región de agregador para recopilar los datos AWS Config de configuración y conformidad. La autorización no es necesaria si se agregan cuentas de origen que forman parte de AWS Organizations.

Un agregador vinculado a un servicio está vinculado a un agregador específico. Servicio de AWS El servicio vinculado establece los datos de configuración y cumplimiento en el ámbito.

Compatibilidad de la región

Actualmente, la agregación de datos de varias cuentas y regiones es compatible en las siguientes regiones:

Nombre de la región	Región	Punto de conexión	Protocolo	
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
Este de EE. UU. (Norte de Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
Oeste de EE. UU. (Norte de California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
Asia-Pacífico (Tailandia)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
México (centro)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Visualización de los datos de conformidad e inventario en el panel de control del agregador para AWS Config

El panel de control de la página de agregadores muestra los datos de configuración de los recursos agregados AWS . Proporciona una descripción general de las reglas, los paquetes de conformidad y sus estados de conformidad.

El panel proporciona el recuento total de AWS recursos. Los tipos de recursos y las cuentas de origen se clasifican por el número más alto de recursos. También proporciona un recuento de las reglas conformes y no conformes y de los paquetes de conformidad. Las reglas no conformes se clasifican según el número más alto de recursos no conformes. Los paquetes de conformidad y las cuentas de origen no conformes se clasifican según el número más alto de reglas no conformes.

Tras la configuración AWS Config, comienza a agregar los datos de las cuentas de origen especificadas en un agregador. Puede tardar unos minutos en mostrarse el estado de conformidad de las reglas.

Uso del panel del agregador

1. Inicie sesión en la AWS Config consola de su casa Consola de administración de AWS y ábrala. https://console.aws.amazon.com/config/
2. Navegue hasta la página Agregadores. En ella aparecen:

- Sus reglas y estados de cumplimiento.
- Sus paquetes de conformidad y sus estados de conformidad.
- Sus AWS recursos y sus datos de configuración.

3. Elija un agregador en el panel de control. Filtre los agregadores por nombre de agregador. Aparecerán los siguientes widgets:

   - Inventario de recursos

     Aquí puede ver los 10 tipos de recursos principales del agregador seleccionado, en orden descendente según el recuento de recursos. Elija el número total de recursos del agregador seleccionado, que aparece entre paréntesis después de Inventario de recursos, para ir a la página de recursos agregados, donde se muestran todos los recursos de un agregador. También puede elegir un tipo de recurso en el widget para ir a la página de recursos agregados, filtrada según el tipo de recurso especificado.

   - Cuentas por recuento de recursos

     Aquí puede ver las cinco cuentas principales del agregador seleccionado, en orden descendente según el recuento de recursos. Elija una cuenta en el widget para ir a la página Recursos, filtrada en función de la cuenta especificada.

   - Reglas no conformes

     Consulte las cinco reglas principales con incumplimiento del agregador seleccionado, en orden descendente según la cantidad de recursos con incumplimiento. Elija una regla en el widget para ir a la página de detalles de la regla especificada. Seleccione Ver todas las reglas no conformes para ir a la página de reglas agregadas, donde se muestran todas las reglas de un agregador.

   - Cuentas por reglas no conformes

     Aquí se muestran las cinco cuentas principales del agregador seleccionado, en orden descendente según el número de reglas no conformes. Elija una cuenta en el widget para ir a la página de reglas agregadas, donde se muestran todas las reglas de un agregador filtradas según la cuenta especificada.

   - Cuentas por paquetes de conformidad no conformes

     Aquí se muestran las cinco cuentas principales del agregador seleccionado, en orden descendente según el número de paquetes de conformidad no conformes. Elija una cuenta en

el widget para ir a la página de paquete de conformidad agregado, donde se muestran todos los paquetes de conformidad de un agregador filtradas según la cuenta especificada.

4. En el panel de navegación izquierdo, elija una de las siguientes opciones del menú desplegable:

   - Panel de cumplimiento

     Aquí se muestran los paneles de cumplimiento automatizados mediante los widgets que resumen la información sobre el cumplimiento de los recursos en el agregador. Se muestran datos como los 10 tipos de recursos principales ordenados por recursos no conformes y los 10 principales paquetes de conformidad en el nivel de cuenta desglosados por reglas no conformes. Para obtener información sobre estos gráficos y tablas, consulte Paneles de cumplimiento.

   - Paquetes de conformidad

     Vea todos los paquetes de conformidad que se crearon y se vincularon a los diferentes Cuentas de AWS dentro de su agregador. La página Paquete de conformidad muestra una tabla con el nombre, la región, el ID de cuenta y el estado de conformidad de cada paquete de conformidad. En esta página, puede elegir un paquete de conformidad y Ver detalles para obtener más información sobre sus normas, recursos y estado de conformidad.

   - Reglas

     Aquí se muestran todas las reglas que se han creado y vinculado a las distintas cuentas de AWS dentro del agregador. La página Reglas muestra una tabla con el nombre, el estado de cumplimiento, la región y la cuenta de cada regla. En esta página, puede elegir una regla y Ver detalles para obtener información, como el agregador, la región, el ID de cuenta y los recursos incluidos en el ámbito.

   - Panel de inventario

     Aquí se muestran los paneles de inventario automatizados mediante los widgets que resumen la información sobre los datos de configuración de los recursos en el agregador. Se muestran datos como los 10 tipos de recursos principales por recuento de recursos y las 10 cuentas principales por recuento de recursos. Para obtener información sobre estos gráficos y tablas, consulte Paneles de inventario.

   - Recursos

     Aquí se muestran todos los recursos registrados y vinculados a las distintas cuentas de AWS dentro del agregador. En la página Recursos, elija un recurso y Ver detalles para ver sus

detalles, las reglas asociadas a él y la configuración actual del recurso. También se muestra información sobre el recurso, como su agregador, región, ID de cuenta, nombre del recurso, tipo de recurso e ID de recurso.

- Autorizaciones

  Aquí puede ver y administrar todas las cuentas actualmente autorizadas o pendientes de autorización. En la página Autorizaciones, seleccione Añadir una autorización para proporcionar acceso a otra cuenta. Seleccione Eliminar la autorización para revocar el acceso desde un ID de cuenta.

> **Note**
>
> Solución de problemas
> Puede aparecer el mensaje Data collection from all source accounts and regions is incomplete en la vista agregada por los siguientes motivos:
>
> - La transferencia de AWS Config reglas y datos de configuración de los AWS recursos que no cumplen con los requisitos está en curso.
> - AWS Config no encuentra reglas que coincidan con el filtro que ha aplicado. Seleccione la cuenta o la región adecuadas e inténtelo de nuevo.
>
> Es posible que este mensaje se muestre en la vista agregada: Data collection from all source accounts and regions is incomplete. You can view the below data only for 24 hours. Se muestra por una de las siguientes razones:
>
> - AWS Config no puede acceder a los detalles de su organización debido a una función de IAM que no es válida. Si el rol de IAM sigue sin ser válido durante más de 24 horas, AWS Config elimina los datos de toda la organización.
> - AWS Config el acceso al servicio está deshabilitado en su organización.

Panel de cumplimiento

Aquí se muestran los paneles de cumplimiento automatizados mediante los widgets que resumen la información sobre el cumplimiento de los recursos en el agregador. El panel muestra solo reglas con resultados de cumplimiento.

> **Note**
>
> Limitaciones
>
> La información del panel de control de conformidad la proporciona la función de consultas avanzadas de AWS Config, y esta función no admite estructuras anidadas ni desempaquetar matrices anidadas. Esto significa que el panel de cumplimiento muestra el cumplimiento general de un recurso y no el estado de cumplimiento de cada regla específica que informa sobre un recurso.
>
> Por ejemplo, si selecciona el elemento de configuración (CI) para el tipo de recurso `AWS::Config::ResourceCompliance`, el panel mostrará los resultados de cumplimiento de todas las reglas que se refieran a ese recurso. Si hay diez reglas que se refieren al recurso, nueve de ellas son COMPLIANT y solo una es NON_COMPLIANT, el cumplimiento general de ese recurso será NON_COMPLIANT.

Compliance Summary By Resources

Muestra un gráfico circular que compara la cantidad de recursos conformes con los recursos no conformes del agregador seleccionado. Pase el ratón sobre el gráfico para ver el número exacto y el porcentaje de recursos conformes y no conformes.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos.

Los 10 tipos de recursos principales ordenados por recursos no conformes

Muestra un gráfico de barras horizontales en el que se comparan hasta diez tipos de recursos del agregador seleccionado en orden descendente según el número de recursos no conformes. Pase el ratón sobre el gráfico para ver el número exacto de recursos no conformes para cada tipo de recurso.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos.

Las 10 cuentas principales ordenadas por recursos no conformes

Las 10 cuentas principales ordenadas por recursos no conformes muestra un gráfico de barras horizontales en el que se comparan hasta diez cuentas del agregador seleccionado en orden

descendente según el número de recursos no conformes. Pase el ratón sobre el gráfico para ver el número exacto de recursos no conformes para cada cuenta.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos.

Las 10 regiones principales ordenadas por recursos no conformes

Muestra un gráfico de barras horizontales en el que se comparan hasta diez regiones donde el agregador seleccionado recopila datos en orden descendente según el número de recursos no conformes. Pase el ratón sobre el gráfico para ver el número exacto de recursos no conformes para cada región.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado.

Los 10 paquetes de conformidad de cuenta principales ordenados por reglas no conformes

Muestra un gráfico de barras horizontales en el que se comparan hasta diez paquetes de conformidad en el nivel de cuenta del agregador seleccionado, en orden descendente según el número de reglas no conformes. Pase el ratón sobre el gráfico para ver el porcentaje de reglas conformes y no conformes para cada paquete de conformidad en el nivel de cuenta.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos.

Los 10 paquetes de conformidad de organización principales ordenados por reglas no conformes

Muestra un gráfico de barras horizontales en el que se comparan hasta diez paquetes de conformidad en el nivel organizativo del agregador seleccionado, en orden descendente según el número de reglas no conformes. Pase el ratón sobre el gráfico para ver el porcentaje de reglas conformes y no conformes para cada paquete de conformidad en el nivel organizativo.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos.

Las 10 cuentas principales ordenadas por reglas no conformes en todos los paquetes de conformidad

Las 10 cuentas principales ordenadas por reglas no conformes en todos los paquetes de conformidad muestra un gráfico de barras horizontales en el que se comparan hasta diez cuentas del agregador seleccionado en orden descendente según el número de reglas no conformes en todos los paquetes de conformidad. Pase el ratón sobre el gráfico para ver el número exacto de reglas no conformes en cada cuenta.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos.

Panel de inventario

Aquí se muestran los paneles de inventario automatizados mediante los widgets que resumen la información sobre los datos de configuración de los recursos en el agregador.

Top 10 resource types by resource count

Muestra un gráfico de barras horizontales en el que se comparan hasta 10 tipos de recursos del agregador seleccionado en orden descendente según el recuento de recursos. Pase el ratón sobre el gráfico para ver el número exacto de recursos para cada tipo de recurso.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos.

Resource count by region

Muestra un gráfico de barras horizontales en el que se comparan hasta 10 regiones donde el agregador seleccionado recopila datos en orden descendente según el recuento de recursos. Pase el ratón sobre el gráfico para ver el número exacto de recursos para cada región.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado.

Top 10 accounts by resource count

Muestra un gráfico de barras horizontales en el que se comparan hasta 10 cuentas del agregador seleccionado en orden descendente según el recuento de recursos. Pase el ratón sobre el gráfico para ver el número exacto de recursos para cada tipo de recurso.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos.

Resource count by Amazon EC2 service resource types

Muestra un gráfico de barras horizontales en el que se comparan tipos de recursos de Amazon EC2 del agregador seleccionado en orden descendente por recuento de recursos. Pase el ratón sobre el gráfico para ver el número exacto de recursos para cada tipo de recurso de Amazon EC2.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos. Para utilizar este gráfico, debe configurar el registro para que guarde los tipos de recursos de Amazon EC2. Para obtener más información, consulte Seleccionar qué registros de recursos. AWS Config

Top 10 EC2 instance types used

Muestra un gráfico de barras horizontales en el que se comparan hasta 10 tipos de instancia de Amazon EC2 del agregador seleccionado en orden descendente por uso. Pase el ratón sobre el gráfico para ver el uso de cada tipo de instancia de EC2.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos. Para utilizar este gráfico, debe configurar el registro para guardar el tipo de recurso de instancia de EC2. Para obtener más información, consulte Recodificación de AWS recursos.

EBS Volume counts by volume type and size

Muestra un gráfico de barras verticales que compara los volúmenes de EBS del agregador seleccionado por recuento de recursos. Pase el ratón sobre el gráfico para ver el recuento y el desglose del tamaño para cada tipo de volumen de EBS.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado

está configurado para recopilar datos. Para utilizar este gráfico, debe configurar el registro de manera que grabe el tipo de recurso de volumen de EC2. Para obtener más información, consulte Seleccionar qué AWS Config registros de recursos.

Number of EC2 instances that are running vs. stopped by type

Muestra un gráfico de barras horizontales en el que se comparan los tipos de instancias de EC2 del agregador seleccionado que se están ejecutando con las instancias de EC2 que se detienen por tipo de instancia. Pase el ratón sobre el gráfico para ver el número exacto de instancias de EC2 detenidas y en ejecución para cada tipo.

Los datos que se muestran dependen de los ajustes del registro de configuración de cada cuenta del agregador seleccionado y de las regiones en las que el agregador seleccionado está configurado para recopilar datos. Para utilizar este gráfico, debe configurar el registro para guardar el tipo de recurso de instancia de EC2. Para obtener más información, consulte Recodificación de AWS recursos.

Creación de agregadores para AWS Config

Puede usar la consola de AWS Config o la AWS CLI para crear los agregadores. Desde AWS Config, puede elegir Añadir los ID de las cuentas individuales o Añadir mi organización desde el lugar en el que desee añadir los datos. Para la AWS CLI, hay dos procedimientos diferentes.

Creating Aggregators (Console)

En la página Agregador, puede crear un agregador especificando los ID de cuenta de origen o la organización y las regiones desde donde desea agregar datos.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Config en https://console.aws.amazon.com/config/home.
2. Vaya a la página Agregadores y elija Crear agregador.
3. Permitir la replicación de datos concede permiso a AWS Config para replicar los datos de las cuentas de origen en una cuenta de agregador.

   Elija Permitir que AWS Config replique datos desde las cuentas de origen en una cuenta de agregador. Debe seleccionar esta casilla de verificación para seguir agregando un agregador.
4. En Nombre del agregador, escriba el nombre del agregador.

El nombre del agregador debe ser nombre único con un máximo de 64 caracteres alfanuméricos. El nombre puede contener guiones y guiones bajos.

5. En Seleccionar cuentas de origen, elija Añadir los ID de las cuentas individuales o Añadir mi organización desde donde desee agregar datos.

> **Note**
>
> Se requiere autorización cuando se utilizan Agregar ID de cuenta individuales para seleccionar las cuentas de origen.

- Si elige Agregar ID de cuenta individuales, puede agregar ID de cuenta individuales para una cuenta de agregador.
  1. Elija Agregar cuentas de origen para añadir los ID de cuenta que desee.
  2. Elija Agregar ID de Cuenta de AWS para agregar manualmente ID de cuenta de Cuenta de AWS separados por comas. Si desea agregar los datos de la cuenta actual, escriba el ID de la cuenta.

     O BIEN

     Elija Cargar un archivo para cargar un archivo (.txt o.csv) con ID de cuenta de Cuenta de AWS separados por comas.
  3. Elija Agregar cuentas de origen para confirmar la opción elegida.
- Si elige Agregar mi organización, puede agregar todas las cuentas de su organización a una cuenta de agregador.

> **Note**
>
> Debe haber iniciado sesión en la cuenta de administración o la de un administrador delegado registrado y todas las características debe estar habilitadas en su organización. Si la persona que llama es una cuenta de administración, AWS Config llama a la API `EnableAwsServiceAccess` para permitir la integración entre AWS Config y AWS Organizations. Si la persona que llama es un administrador delegado registrado, AWS Config llama a la API `ListDelegatedAdministrators` para comprobar si la persona que llama es un administrador delegado válido.

Asegúrese de que la cuenta de administración registre un administrador delegado para el nombre de la entidad principal de servicio de AWS Config (onfig.amazonaws.com) antes de que el administrador delegado cree un agregador. Para registrar un administrador delegado, consulte Registro de un administrador delegado para AWS Config.

Debe asignar un rol de IAM que permita a AWS Config llamar a API de solo lectura para su organización.

1. Seleccione Elegir un rol de su cuenta para seleccionar un rol de IAM existente.

> **Note**
>
> En la consola de IAM, asocie la política administrada de `AWSConfigRoleForOrganizations` a su rol de IAM. Asociar esta política permite a AWS Config llamar a las API AWS Organizations, `DescribeOrganization` y `ListAWSServiceAccessForOrganization` de `ListAccounts`. De forma predeterminada, `config.amazonaws.com` se especifica automáticamente como entidad de confianza.

2. Elija Crear un rol y escriba el nombre del rol de IAM para crear el rol de IAM.

6. En Regiones, elija las regiones cuyos datos desee agregar.
   - Seleccione una o varias regiones, o todas las Regiones de AWS.
   - Seleccione Incluir futuras Regiones de AWS para agregar datos de todas las Regiones de AWS futuras en las que esté habilitada la agregación de datos de varias cuentas y regiones.
7. Elija Guardar. AWS Config muestra el agregador.

Creating Aggregators using Individual Accounts (AWS CLI)

1. Abra un símbolo del sistema o una ventana de terminal.
2. Escriba el siguiente comando para crear un agregador denominado **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

Para `account-aggregation-sources`, introduzca una de las siguientes opciones:

- Escriba una lista separada por comas de los ID de Cuenta de AWS cuyos datos desea agregar. Encierre los ID de cuenta entre corchetes y asegúrese de aplicar escape a las comillas (por ejemplo, `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\", \"AccountID3\"],\"AllAwsRegions\": true}]"`).
- También puede cargar un archivo JSON con los ID de Cuenta de AWS separados por comas. Cargue el archivo utilizando la siguiente sintaxis: `--account-aggregation-sources MyFilePath/MyFile.json`

  El archivo JSON debe tener el siguiente formato:

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. Pulse Intro para ejecutar el comando.

   Debería ver una salida similar a esta:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
```

```
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Creating Aggregators using AWS Organizations (AWS CLI)

Antes de iniciar este procedimiento, debe haber iniciado sesión en la cuenta de administración o la de un administrador delegado registrado y todas las características debe estar habilitadas en su organización.

> **Note**
>
> Asegúrese de que la cuenta de administración registre un administrador delegado con los siguientes nombres de la entidad principal de servicio de AWS Config (`config.amazonaws.com` y `config-multiaccountsetup.amazonaws.com`) antes de que el administrador delegado cree un agregador. Para registrar un administrador delegado, consulte Registro de un administrador delegado para AWS Config.

1. Abra un símbolo del sistema o una ventana de terminal.
2. Si no ha creado un rol de IAM para su agregador de AWS Config, introduzca el siguiente comando:

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":\"\",\"Effect
\":\"Allow\",\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action
\":\"sts:AssumeRole\"}]}" --description "Role for organizational AWS Config
 aggregator"
```

> **Note**
>
> Copie el nombre de recurso de Amazon (ARN) desde este rol de IAM para utilizarlo al crear su agregador de AWS Config. Puede encontrar los ARN en el objeto de respuesta.

3. Si no ha asociado ninguna política a su rol de IAM, adjunte la política gestionada de AWSConfigRoleForOrganizations o introduzca el siguiente comando:

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17",       "Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAw
```

4. Introduzca el siguiente comando para crear un agregador denominado **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. Pulse Intro para ejecutar el comando.

   Debería ver una salida similar a esta:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Registro de un administrador delegado para AWS Config

Los administradores delegados son cuentas de una AWS organización determinada a las que se conceden privilegios administrativos adicionales para un AWS servicio específico. Para obtener más información, consulte Delegated administrator en la Guía del usuario de AWS Organizations . Para registrar un administrador delegado, debe usar la AWS CLI .

Registro de un administrador delegado

1. Inicie sesión con las credenciales de la cuenta de administración.
2. Abra un símbolo del sistema o una ventana de terminal.
3. Introduzca el siguiente comando para habilitar el acceso al servicio como administrador delegado para que su organización pueda implementar y administrar AWS Config las reglas y los paquetes de conformidad en toda la organización:

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. Introduzca el siguiente comando para habilitar el acceso a los servicios como administrador delegado de su organización a fin de agregar AWS Config datos en toda la organización:

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. Para comprobar si la activación del acceso al servicio se ha completado, introduzca el siguiente comando y pulse Intro para ejecutarlo.

```
aws organizations list-aws-service-access-for-organization
```

Debería ver una salida similar a esta:

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
```

```
    ]
}
```

6. A continuación, introduzca el siguiente comando para registrar una cuenta de miembro como administrador delegado para AWS Config.

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

and

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. Para comprobar si se ha completado el registro del administrador delegado, introduzca el siguiente comando desde la cuenta de administración y pulse Intro para ejecutar el comando.

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

and

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

Debería ver una salida similar a esta:

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::ManagementAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
```

```
}
```

Edición de agregadores para AWS Config

Puede usar la consola de AWS Config o la AWS CLI para editar agregadores.

Editing Aggregators (Console)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Config en https://console.aws.amazon.com/config/home.
2. Vaya a la página Agregador y seleccione el nombre del agregador.
3. Elija Acciones y, a continuación, elija Editar.
4. Utilice las secciones de la página Editar agregador para cambiar las cuentas de origen, los roles de IAM o las regiones para el agregador.

   > **Note**
   >
   > No puede cambiar el tipo de origen de cuentas individuales a organización y viceversa.

5. Seleccione Save.

Editing Aggregators (AWS CLI)

1. Puede utilizar el comando `put-configuration-aggregator` para actualizar o editar un agregador de configuración.

   Introduzca el siguiente comando para añadir un ID de cuenta nuevo a **`MyAggregator`**:

   ```
   aws configservice put-configuration-aggregator --configuration-aggregator-name
    MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
   \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
   ```

2. En función de su cuenta de origen, debería ver un resultado similar al siguiente:

   Para cuentas individuales

   ```
   {
   ```

```
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

O BIEN

Para una organización

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Eliminación de agregadores para AWS Config

Puede usar la consola de AWS Config o la AWS CLI para eliminar agregadores.

Deleting Aggregators (Console)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Config en https://console.aws.amazon.com/config/home.
2. Vaya a la página Agregador y seleccione el nombre del agregador.
3. Elija Acciones y, a continuación, elija Eliminar.

   Se muestra un mensaje de advertencia. Al eliminar un agregador, se pierden todos los datos agregados. No puede recuperar estos datos, pero los datos de las cuentas de origen no se verán afectados.
4. Elija Eliminar para confirmar la opción elegida.

Deleting Aggregators (AWS CLI)

Escriba el siguiente comando:

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

Si se ejecuta correctamente, el comando no muestra ninguna salida adicional.

Autorización de las cuentas agregadoras para recopilar datos de AWS Config configuración y cumplimiento

La autorización se refiere a los permisos que concedes a una cuenta y región de agregador para recopilar tus datos AWS Config de configuración y conformidad. La autorización no es necesaria si se agregan cuentas de origen que forman parte de AWS Organizations. Puede usar la AWS Config consola o la AWS CLI para autorizar las cuentas de los agregadores.

Temas

- Consideraciones
- Autorización de envío

Consideraciones

Hay dos tipos de agregadores: el agregador de cuentas individuales y el agregador de la organización

En el caso de un agregador de cuentas individuales, se requiere la autorización de todas las cuentas y regiones de origen que quiera incluir, tanto las cuentas externas y las regiones como las cuentas de miembros de la organización y las regiones.

En el caso de un agregador de organizaciones, no se requiere autorización para las regiones de cuentas de los miembros de la organización, ya que la autorización está integrada en el AWS Organizations servicio.

Los agregadores no se activan automáticamente AWS Config en tu nombre

AWS Config debe estar habilitado en la cuenta y la región de origen para cualquiera de los tipos de agregadores para que AWS Config los datos se generen en la cuenta y la región de origen.

Autorización de envío

Adding Authorization (Console)

Puede añadir una autorización para conceder permiso a las cuentas agregadoras y a las regiones para recopilar datos de AWS Config configuración y conformidad.

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.
2. Vaya a la página Authorizations (Autorizaciones) y elija Add authorization (Añadir autorización).
3. En Aggregator account (Cuenta de agregador), escriba el ID de 12 dígitos de la cuenta de agregador.
4. En Región del agregador, elija las Regiones de AWS en las que la cuenta de agregador tiene permiso para recopilar datos de configuración y conformidad de AWS .
5. Elija Add authorization (Añadir autorización) para confirmar la opción elegida.

   AWS Config muestra una cuenta del agregador, una región y un estado de autorización.

> **Note**
>
> También puede añadir autorizaciones a las cuentas y regiones del agregador de forma programática mediante plantillas de muestra. CloudFormation Para obtener más información, consulte AWS::Config::AggregationAuthorization en la Guía del usuario de CloudFormation .

Authorizing a Pending Request (Console)

Si tiene una solicitud de autorización pendiente para una cuenta de agregador existente, verá el estado de la solicitud en la página Autorizaciones. Puede autorizar una solicitud pendiente desde esta página.

1. Elija la cuenta de agregador que desee autorizar y, a continuación, Autorizar.

   Aparece un mensaje de confirmación para confirmar que desea conceder permiso a la cuenta agregadora para recopilar AWS Config datos de esta cuenta.
2. Vuelva a seleccionar Autorizar para confirmar que desea conceder el permiso a la cuenta del agregador.

   El estado de autorización cambia de Requesting for authorization (Autorización solicitada) a Authorized (Autorizada).

Periodo de aprobación de la autorización

Se requiere la aprobación de la autorización para agregar cuentas de origen a un agregador de cuentas individual. Una solicitud de aprobación de autorización pendiente estará disponible durante siete días después de que un agregador de cuentas individual agregue una cuenta de origen.

Adding Authorization (AWS CLI)

1. Abra un símbolo del sistema o una ventana de terminal.
2. Introduzca el siguiente comando:

```
aws configservice put-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

3. Debería ver una salida similar a esta:

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

Eliminar la autorización de las cuentas de agregador para recopilar datos AWS Config de configuración y cumplimiento

La autorización se refiere a los permisos que concedes a una cuenta y región de agregador para recopilar tus datos AWS Config de configuración y conformidad. La autorización no es necesaria si se agregan cuentas de origen que forman parte de AWS Organizations. Puede usar la AWS Config consola o la AWS CLI para eliminar las autorizaciones.

Temas

- Consideraciones
- Eliminación de la autorización

Consideraciones

Hay dos tipos de agregadores: el agregador de cuentas individuales y el agregador de la organización

En el caso de un agregador de cuentas individuales, se requiere la autorización de todas las cuentas y regiones de origen que quiera incluir, tanto las cuentas externas y las regiones como las cuentas de miembros de la organización y las regiones.

En el caso de un agregador de organizaciones, no se requiere autorización para las regiones de cuentas de los miembros de la organización, ya que la autorización está integrada en el AWS Organizations servicio.

Los agregadores no se activan automáticamente AWS Config en su nombre

AWS Config debe estar habilitado en la cuenta y la región de origen para cualquiera de los tipos de agregadores para que AWS Config los datos se generen en la cuenta y la región de origen.

Eliminación de la autorización

Deleting Authorization (Console)

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.
2. Elija la cuenta de agregador cuya autorización desee eliminar y, a continuación, Eliminar.

   Se muestra un mensaje de advertencia. Al eliminar esta autorización, AWS Config los datos dejarán de compartirse con la cuenta del agregador.
3. Elija Eliminar para confirmar la opción elegida.

   Se ha eliminado la cuenta de agregador.

Deleting Authorization (AWS CLI)

Introduzca el siguiente comando:

```
aws configservice delete-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

Si se ejecuta correctamente, el comando no muestra ninguna salida adicional.

Visualización de agregadores para AWS Config

Puede usar la consola de AWS Config o la AWS CLI para ver agregadores.

Viewing Aggregators (Console)

Para ver los paquetes de conformidad en la Consola de administración de AWS, consulte Aggregator Dashboard.

Viewing Aggregators (AWS CLI)

1. Escriba el siguiente comando:

```
aws configservice describe-configuration-aggregators
```

2. En función de su cuenta de origen, debería ver un resultado similar al siguiente:

   Para cuentas individuales

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn":
 "arn:aws:config:Region:AccountID:config-aggregator/config-aggregator-floqpus3",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

   O BIEN

   Para una organización

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
```

```
        },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Solución de problemas de agregación de datos multicuenta y multirregión para AWS Config

AWS Config es posible que no agregue datos de las cuentas de origen por uno de los siguientes motivos:

Si ocurre esto	Haga lo siguiente
AWS Config no está habilitado en la cuenta de origen para las cuentas de una organización.	AWS Config Actívela en la cuenta de origen y autorice a la cuenta agregadora a recopilar datos.
No se ha concedido autorización a una cuenta de agregador.	Inicie sesión en la cuenta de origen y autorice a la cuenta del agregador para recopilar datos AWS Config .
Es posible que haya un problema temporal que impida la acumulación de datos.	La acumulación de datos está sujeta a retrasos. Espere unos minutos.

AWS Config es posible que no agregue datos de una organización por uno de los siguientes motivos:

Si ocurre esto	Haga lo siguiente
AWS Config no puede acceder a los detalles de su organización debido a una función de IAM no válida.	Cree un rol de IAM o seleccione un rol de IAM válido en la lista de roles de IAM.

Si ocurre esto	Haga lo siguiente
	Note Si el rol de IAM no es válido durante más de 7 días, AWS Config elimina los datos de toda la organización.
AWS Config el acceso al servicio está deshabilitado en su organización.	Puede habilitar la integración entre AWS Config y AWS Organizations a través de la `EnableAWSServiceAccess` API. Si eliges Añadir mi organización en la consola, AWS Config se habilita automáticamente la integración entre AWS Config y AWS Organizations.
AWS Config no puede acceder a los detalles de su organización porque no todas las funciones están habilitadas en su organización.	Activa todas las funciones de AWS Organizations la consola.
Los cambios organizativos, como añadir una cuenta, eliminar una cuenta, habilitar el acceso a los servicios y deshabilitar el acceso a los servicios, no se actualizan inmediatamente en las regiones de Medio Oriente (Bahréin) y Asia Pacífico (Hong Kong).	Los cambios organizativos están sujetos a un retraso de 2 horas. Espere 2 horas para ver todos los cambios en la organización.

Consulta del estado de la configuración actual de AWS los recursos con AWS Config

Presentamos una función de vista previa para consultas avanzadas que permite utilizar las capacidades de la inteligencia artificial generativa (IA generativa) para introducir las solicitudes en un lenguaje sencillo y convertirlas en un ready-to-use formato de consulta. Para obtener más información, consulte Procesador de consultas en lenguaje natural para consultas avanzadas.

Puede utilizarla AWS Config para consultar el estado de configuración actual de AWS los recursos en función de las propiedades de configuración de una sola cuenta y región o de varias cuentas y regiones. Puede realizar consultas basadas en propiedades en función de los metadatos del estado actual de los AWS recursos en una lista de recursos compatibles AWS Config . Para obtener más información sobre la lista de tipos de recursos compatibles, consulte Tipos de recursos compatibles para consultas avanzadas.

La característica Consultas avanzadas proporciona un único punto de conexión de consultas, así como un lenguaje de consultas, para obtener los metadatos del estado actual de los recursos, sin necesidad de realizar llamadas a la API “describe” específicas de los servicios. Puede usar agregadores de configuración para ejecutar las mismas consultas desde una cuenta central en varias cuentas y regiones. AWS

Temas

- Características
- Componentes de consulta para AWS Config
- Consulta mediante el editor de consultas SQL para AWS Config (consola)
- Consulta mediante el editor de consultas SQL para AWS Config (AWS CLI)
- Procesador de consultas en lenguaje natural para consultas AWS Config avanzadas
- Consultas de ejemplo para AWS Config
- Ejemplos de consultas de relación para AWS Config
- Limitaciones
- Comportamiento del notation/IP rango CIDR para consultas avanzadas
- Comportamiento de múltiples propiedades en una matriz para consultas avanzadas

- Compatibilidad de la región

Características

AWS Config utiliza un subconjunto de la `SELECT` sintaxis del lenguaje de consultas estructurado (SQL) para realizar consultas y agregaciones basadas en propiedades en los datos del elemento de configuración (CI) actual. Las consultas varían en complejidad, desde coincidencias con identificadores de and/or recursos de etiquetas hasta consultas más complejas, como la visualización de todos los buckets de Amazon S3 que tienen deshabilitado el control de versiones. Esto le permite consultar exactamente el estado actual del recurso que necesita sin realizar llamadas a la API específicas del AWS servicio.

Admite funciones de agregación como, por ejemplo, `AVG`, `COUNT`, `MAX`, `MIN` y `SUM`.

Puede utilizar las consultas avanzadas para tareas de:

- Administración de inventarios; por ejemplo, para recuperar una lista de las instancias de Amazon EC2 que tienen un tamaño determinado.
- Seguridad e inteligencia operativa; por ejemplo, para recuperar una lista de los recursos que tienen una propiedad de configuración específica habilitada o deshabilitada.
- Optimización de costos; por ejemplo, para identificar una lista de los volúmenes de Amazon EBS que no están asociados a ninguna instancia EC2.
- Datos de conformidad; por ejemplo, para recuperar una lista de todos los paquetes de conformidad y su estado de conformidad.

Para obtener información sobre cómo utilizar el lenguaje de consultas AWS SQL, consulte ¿Qué es SQL (lenguaje de consulta estructurado)? .

Componentes de consulta para AWS Config

Los componentes de SQL `SELECT` para consultas avanzadas de AWS Config son los siguientes.

Sinopsis

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
```

```
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

Parámetros

[WHERE condition]

Filtra los resultados de acuerdo con el valor de `condition` que especifique.

Operadores de comparación

- = (es igual a)
- `IN` (lista de miembros)
- `BETWEEN` (comprobación de rango)

Operadores lógicos

- `AND`
- `OR`
- `NOT`

[GROUP BY propiedad]

Agrega el conjunto de resultados en grupos de filas cuyo valor de la propiedad especificada coincide.

La cláusula GROUP BY es aplicable en las agregaciones.

[ORDER BY propiedad [ASC | DESC] [, propiedad [ASC | DESC] ...]]

Ordena un conjunto de resultados por una o varias salidas `properties`.

Cuando la cláusula contiene varias propiedades, el conjunto de resultados se ordena según la primera `property`, a continuación, de acuerdo con la segunda `property` para las filas cuyo valor coincide para la primera propiedad, etc.

Ejemplos

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

Consulta mediante el editor de consultas SQL para AWS Config (consola)

Presentamos una función de vista previa para consultas avanzadas que permite utilizar las capacidades de inteligencia artificial generativa (IA generativa) para introducir solicitudes en un lenguaje sencillo y convertirlas en un ready-to-use formato de consulta. Para obtener más información, consulte Procesador de consultas en lenguaje natural para consultas avanzadas.

Puede utilizar consultas de AWS muestra o puede crear su propia consulta, denominadas consultas personalizadas.

Consideraciones

Requisitos previos

Si utiliza una de las siguientes políticas AWS gestionadas, dispondrá de los permisos necesarios para ejecutar y guardar una consulta: AWSServiceRoleForConfig(función vinculada a un servicio) o AWS_C OnFigrole.

De lo contrario, debe tener los permisos incluidos en la política administrada. AWSConfigUserAccess AWS

Lista de propiedades que puede consultar

Encontrará una lista actualizada de propiedades y sus tipos de datos en GitHub.

Consultas avanzadas y agregadores

Para ejecutar una consulta en un agregador, cree un agregador. Para obtener más información, consulte Creación de agregadores para AWS Config.

Si ya tiene configurado un agregador, en el ámbito de la consulta, elija el agregador para ejecutar una consulta avanzada en ese agregador. Al seleccionar un agregador, considere agregar el Cuenta de AWS ID y la AWS región en la declaración de consulta para ver esa información en los resultados.

Utilice un AWS ejemplo de consulta

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.

2. Elija Consultas avanzadas en el panel de navegación izquierdo para consultar las configuraciones de recursos de una sola cuenta y región o de varias cuentas y regiones.
3. En la página Consultas avanzadas, elija una consulta adecuada de la lista de consultas. Puede filtrar una lista de consultas por nombre, descripción, creador o etiquetas. Para filtrar las consultas de AWS , seleccione Creador e introduzca AWS. La consulta que seleccione se muestra en el editor de consultas de SQL. Puede editar la consulta seleccionada para adaptarla a sus necesidades.
4. Para guardar esta consulta en una consulta nueva, seleccione Guardar como.
   - En el campo Nombre de la consulta, actualice el nombre de la consulta.
   - En el campo Descripción, actualice la descripción de la consulta.
   - Introduzca hasta 50 etiquetas únicas para esta consulta.
   - Seleccione Save.
5. Elija Ejecutar. Los resultados de la consulta aparecen en la tabla que se muestra debajo del editor de consultas.
6. Elija Exportar como para exportar los resultados de la consulta en formato CSV o JSON.

Creación de una consulta personalizada

1. Inicia sesión en la AWS Config consola Consola de administración de AWS y ábrela en https://console.aws.amazon.com/config/casa.
2. Elija Consultas avanzadas en el panel de navegación izquierdo para consultar las configuraciones de recursos de una sola cuenta y región o de varias cuentas y regiones.
3. Para crear su propia consulta, elija Nueva consulta.

   Para ver o editar una consulta personalizada, puede filtrar una consulta por nombre, descripción, creador o etiquetas. Para filtrar las consultas personalizadas, elija Creador e introduzca Personalizado.
4. En la página Editor de consultas, cree su propia consulta para esta cuenta y región. También puede seleccionar un agregador adecuado para crear una consulta para varias cuentas y regiones.
5. Si desea realizar cambios en esta consulta, edítela. Para guardar esta consulta, elija Guardar consulta.
   - En el campo Nombre de la consulta, actualice el nombre de la consulta.

- En el campo Descripción, actualice la descripción de la consulta.
- Introduzca hasta 50 etiquetas únicas para esta consulta.
- Seleccione Save.

6. Elija Ejecutar. Los resultados de la consulta aparecen en la tabla que se muestra debajo del editor de consultas.
7. Elija Exportar como para exportar los resultados de la consulta en formato CSV o JSON.

Consulta mediante el editor de consultas SQL para AWS Config (AWS CLI)

Se AWS CLI trata de una herramienta unificada para gestionar sus AWS servicios. Con solo descargar y configurar una herramienta, puede controlar varios AWS servicios desde la línea de comandos y utilizar scripts para automatizarlos. Para obtener más información AWS CLI e instrucciones sobre cómo instalarlas AWS CLI , consulte lo siguiente en la Guía del AWS Command Line Interface usuario.

- AWS Command Line Interface Guía del usuario
- Configuración inicial de la AWS Command Line Interface

Si es necesario, introdúzcalo `aws configure` para configurar el AWS CLI uso de una AWS región en la que estén disponibles las consultas avanzadas.

Consideraciones

Requisitos previos

Si utiliza una de las siguientes políticas AWS gestionadas, dispondrá de los permisos necesarios para ejecutar y guardar una consulta: AWSServiceRoleForConfig(función vinculada al servicio) o AWS_C OnFigrole.

De lo contrario, debe tener los permisos incluidos en la política administrada. AWSConfigUserAccess AWS

Lista de propiedades que puede consultar

Encontrará una lista actualizada de propiedades y sus tipos de datos en GitHub.

Consultas avanzadas y agregadores

Para ejecutar una consulta en un agregador, cree un agregador. Para obtener más información, consulte Creación de agregadores para AWS Config.

Si ya tiene configurado un agregador, en el ámbito de la consulta, elija el agregador para ejecutar una consulta avanzada en ese agregador. Al seleccionar un agregador, considere agregar el Cuenta de AWS ID y la AWS región en la declaración de consulta para ver esa información en los resultados.

Consulta de los datos de configuración de los recursos

Para consultar los datos de configuración de recursos mediante el editor de consultas (AWS CLI) para una sola cuenta y región

1. Abra un símbolo del sistema o una ventana de terminal.
2. Introduzca el siguiente comando para hacer consultas en los datos de configuración de recursos.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

En función de la consulta, el resultado tiene un aspecto similar al siguiente:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

Para consultar los datos de configuración de recursos mediante el editor de consultas (AWS CLI) para varias cuentas y regiones

1. Abra un símbolo del sistema o una ventana de terminal.
2. Introduzca el siguiente comando para hacer consultas en los datos de configuración de recursos.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

En función de la consulta, el resultado tiene un aspecto similar al siguiente:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> Si utiliza los tipos de recursos `AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role` y `AWS::IAM::Policy` en una consulta avanzada, use `awsRegion = 'global'`.

Guardar una consulta

1. Abra un símbolo del sistema o una ventana de terminal.
2. Introduzca el siguiente comando para guardar una consulta.

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. En función de la consulta, el resultado tiene un aspecto similar al siguiente:

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` es opcional. Al pasar las etiquetas, ni `list-stored-queries` ni `get-stored-query` devolverán las etiquetas guardadas. Debe utilizar `list-tag-for-resources` para recuperar las etiquetas asociadas a una consulta guardada. `--description` es opcional al crear o actualizar una consulta.

Ver todas las consultas guardadas

1. Introduzca el siguiente comando para ver la lista de todas las consultas guardadas.

```
aws configservice list-stored-queries
```

2. En función de la consulta, el resultado tiene un aspecto similar al siguiente:

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
```

```
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
    ]
}
}
```

Obtener detalles de una consulta guardada

1. Introduzca el siguiente comando para obtener detalles sobre una consulta guardada específica.

```
aws configservice get-stored-query --query-name cli-test
```

2. En función de la consulta, el resultado tiene un aspecto similar al siguiente:

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

Eliminar una consulta guardada

- Introduzca el siguiente comando para eliminar una consulta guardada.

```
aws configservice delete-stored-query --query-name cli-test
```

Si se ejecuta correctamente, el comando no muestra ninguna otra salida.

Procesador de consultas en lenguaje natural para consultas AWS Config avanzadas

> **Note**
>
> La versión preliminar pública de AWS Config Natural Language Query Processor se suspenderá el 15 de enero de 2026. Además, puede conversar sobre sus AWS recursos mediante instrucciones en lenguaje natural con Amazon Q Developer. Para obtener más información, consulte Conversación sobre sus recursos con Amazon Q Developer.

El procesador de consultas en lenguaje natural para consultas avanzadas utiliza Amazon Bedrock, una tecnología de inteligencia artificial generativa (IA generativa) que permite introducir solicitudes en un lenguaje sencillo y convertirlas en un formato de consulta. ready-to-use Con el procesador de consultas en lenguaje natural, puede realizar consultas en su organización Cuenta de AWS o en toda la organización. AWS

Una petición puede ser una pregunta o una afirmación. Por ejemplo, puede introducir peticiones como “¿Qué equilibradores de carga se han creado después del 1 de enero de 2024?” y “Enumera todas las funciones de Lambda que ejecuten Nod.js 16”.

Consideraciones

El procesador de consultas en lenguaje natural no puede llevar a cabo las siguientes acciones:

- Generar consultas desde idiomas que no sean el inglés.
- Generar consultas a partir de peticiones que no estén relacionadas con consultas avanzadas.
- Generar consultas a partir de peticiones con más de 1000 caracteres.
- Generar consultas a partir de correcciones de seguimiento o de sesiones anteriores.
- Explicar el código que se ha generado.

Consultas mediante el procesador de consultas en lenguaje natural

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.

2. Elija Consultas avanzadas en el panel de navegación izquierdo para consultar las configuraciones de recursos de una sola cuenta y región o de varias cuentas y regiones.
3. En la página Consultas avanzadas, elija Nueva consulta para ir al editor de consultas.
   - (Opcional) Para ejecutar una consulta en un agregador, cree un agregador. Para obtener más información, consulte Creación de agregadores para AWS Config.
   - Si ya tiene configurado un agregador, en el ámbito de la consulta, elija el agregador para ejecutar una consulta avanzada en él. Al seleccionar un agregador, considere agregar el Cuenta de AWS ID y la AWS región en la declaración de consulta para ver esa información en los resultados.
4. En el editor de consultas, vaya a la sección Procesador de consultas de lenguaje natural. Introduzca una petición con lenguaje sencillo y seleccione Generar. Para ver ejemplos, consulte Ejemplos de peticiones.
5. Tras generar una consulta, puede seleccionar Copiar (equivalente a Ctrl+C) para copiar la consulta en el portapapeles, o bien elegir Rellenar en el editor. Si se rellena con el editor, puede editar la consulta generada para adaptarla a sus necesidades.
6. Para guardar esta consulta en una consulta nueva, seleccione Guardar como.
   - En el campo Nombre de la consulta, actualice el nombre de la consulta.
   - En el campo Descripción, actualice la descripción de la consulta.
   - Introduzca hasta 50 etiquetas únicas para esta consulta.
   - Seleccione Save.
7. Elija Ejecutar. Los resultados de la consulta aparecen en la tabla que se muestra debajo del editor de consultas.
8. Elija Exportar como para exportar los resultados de la consulta en formato CSV o JSON.

> **Note**
>
> Los resultados de la consulta están paginados. Al elegir exportar, se exportan hasta 500 resultados.
> También puede utilizar el APIs para recuperar todos los resultados. Los resultados se paginan y se pueden recuperar 100 resultados a la vez.

Ejemplos de peticiones

Estas son algunas peticiones y consultas generadas que puede usar como ejemplos.

Example: ¿Qué equilibradores de carga se han creado a partir del 1 de enero de 2024?

Petición: What load balancers were created after January 1, 2024?

Consulta generada:

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: ¿Qué instancias de bases de datos de RDS son de acceso público?

Petición: Which of my RDS database instances are publicly accessible?

Consulta generada:

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: ¿Cuántas instancias de EC2 se han creado en el último año?

Petición: How many EC2 instances were created in last one year?

Consulta generada:

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: ¿Cuántas instancias de EC2 tengo en cada una de mis Cuentas de AWS?

Petición: How many EC2 instances do I have in each of my Cuentas de AWS?

Consulta generada:

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: ¿Qué funciones de IAM incluyen la política gestionada AdministratorAccess ?

Petición: Which IAM roles have the managed policy AdministratorAccess attached?

Consulta generada:

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: Volúmenes de EBS sin cifrado

Petición: EBS volumes without encryption

Consulta generada:

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: Dime cuáles son los recursos no conformes

Petición: Get noncompliant resources

Consulta generada:

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: Enumera todas las funciones de Lambda que ejecuten Nod.js 16.

Petición: List all my lambda function that is running node js 16

Consulta generada:

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: ¿Qué certificados ACM caducan en los próximos 30 días?

Petición: What ACM certificates expire the next 30 days?

Consulta generada:

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> Los tiempos de la consulta generada dependen del momento en el que se introduzca la petición.

Aportación de comentarios

Puede proporcionar comentarios generales sobre el procesador de consultas en lenguaje natural o sobre una consulta generada específica.

Comentarios sobre el procesador de consultas en lenguaje natural

Seleccione el botón Enviar comentarios, encima del procesador de consultas en lenguaje natural, a la derecha. Puede indicar su grado de satisfacción o insatisfacción y enviar comentarios sobre cómo AWS Config puede hacer que la consulta en lenguaje natural sea más útil.

> **Note**
>
> No divulgue ninguna información personal, confidencial o de importancia comercial.

Comentarios sobre una consulta generada específica

Para enviar comentarios acerca de una consulta generada, pulse el botón con el pulgar hacia arriba o hacia abajo que aparece debajo de la consulta generada.

Compatibilidad de la región

El procesador de consultas en lenguaje natural es compatible con las siguientes regiones.

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Norte de Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Consultas de ejemplo para AWS Config

Consulte los siguientes ejemplos de consultas.

Query to list all EC2 instances with AMI ID ami-12345

Consulta:

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

Resultados:

```
{
    "QueryInfo": {
```

```
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}"
    ]
```

```
}
```

Query for count of resources grouped by their AWS Config rules compliance status

Consulta:

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

Resultados:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

Consulta:

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
```

```
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

Resultados:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

Consulta:

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

Resultados:

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

Consulta:

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

Resultados:

```
{
    "Results": [
```

```
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
```

```
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

Ejemplos de consultas de relación para AWS Config

Consulte el siguiente ejemplo de consultas de relación.

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

OR

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

Limitaciones

> **Note**
>
> La consulta avanzada no admite la consulta de recursos que no se hayan configurado para que los grabe el grabador de configuración. AWS Config crea elementos de configuración (CIs) `configurationItemStatus` cuando se descubre un recurso pero no está configurado para que el grabador de configuración lo grabe. `ResourceNotRecorded` Si bien un agregador los agregará CIs, la consulta avanzada no admite consultas CIs con. `ResourceNotRecorded` Actualice la configuración del grabador para permitir el registro de los tipos de recursos que desee consultar.

Dado que es un subconjunto del comando `SELECT` de SQL, la sintaxis de consultas tiene las siguientes limitaciones:

- No se admiten las palabras clave `ALL`, `AS`, `DISTINCT`, `FROM`, `HAVING`, `JOIN` ni `UNION` en una consulta. No se admiten consultas con valores `NULL`.
- No se admiten instrucciones complejas de `CASE` para crear un campo de prioridad directamente en la consulta.
- No se admite la consulta de recursos de terceros. Los recursos de terceros recuperados mediante consultas avanzadas tendrán el campo de configuración establecido como `NULL`.
- No se admite la posibilidad de desempaquetar estructuras anidadas (como etiquetas) con consultas SQL.
- No se admite la consulta de recursos eliminados. Para descubrir los recursos eliminados, consulte Buscar recursos descubiertos por. AWS Config
- La sintaxis abreviada del comando `SELECT` para todas las columnas (es decir `SELECT *`) selecciona únicamente las propiedades escalares de nivel superior de un CI. Las propiedades escalares devueltas son `accountId`, `awsRegion`, `arn`, `availabilityZone`, `configurationItemCaptureTime`, `resourceCreationTime`, `resourceId`, `resourceName`, `resourceType` y `version`.
- Limitaciones de los caracteres comodín:
  - Los caracteres comodín solo se admiten para los valores de las propiedades, no para las claves de las propiedades (por ejemplo, se admite `...WHERE someKey LIKE 'someValue%'`, pero no `...WHERE 'someKey%' LIKE 'someValue%'`).

- Solo se admiten los caracteres comodín como sufijo (por ejemplo, se admiten `...LIKE 'AWS::EC2::%'` y `...LIKE 'AWS::EC2::_'`, pero no `...LIKE '%::EC2::Instance'` y `...LIKE '_::EC2::Instance'`).
- Las coincidencias con caracteres comodín deben ser de tres caracteres como mínimo (por ejemplo, `...LIKE 'ab%'` y `...LIKE 'ab_'` no se permiten pero `...LIKE 'abc%'` y `...LIKE 'abc_'` sí).

> **Note**
>
> El "_" (subrayado único) también se considera un comodín.

- Límites de las agregaciones:
  - Las funciones de agregación únicamente pueden aceptar un solo argumento o propiedad.
  - Las funciones de agregación no pueden tomar otras funciones como argumentos.
  - `GROUP BY` con una cláusula `ORDER BY` que haga referencia a funciones de agregación puede contener solamente una propiedad única.
  - Para todas las demás agregaciones, las cláusulas `GROUP BY` pueden contener hasta tres propiedades.
  - La paginación es compatible con todas las consultas agregadas, excepto cuando la cláusula `ORDER BY` tiene una función de agregación. Por ejemplo, `GROUP BY X, ORDER BY Y` no funciona si `Y` es una función de agregación.
  - No se admiten las cláusulas `HAVING` en las agregaciones.
- Limitaciones de los identificadores no coincidentes:

  Los identificadores no coincidentes son propiedades que tienen la misma ortografía pero distintas mayúsculas y minúsculas. La consulta avanzada no admite el procesamiento de consultas que contengan identificadores no coincidentes. Por ejemplo:

  - Dos propiedades que tienen exactamente la misma ortografía pero con mayúsculas y minúsculas diferentes (`configuration.dbclusterIdentifier` y `configuration.dBClusterIdentifier`).
  - Dos propiedades en las que una es un subconjunto de la otra y tienen mayúsculas diferentes (`configuration.ipAddress` y `configuration.ipaddressPermissions`).

Comportamiento del notation/IP rango CIDR para consultas avanzadas

La notación CIDR se convierte en rangos de IP para la búsqueda.

Esto significa que `"="` y `"BETWEEN"` buscan cualquier rango que incluya la IP proporcionada, en lugar de buscar uno exacto.

Para buscar un rango de IP exacto, debe agregar condiciones adicionales para excluir IPs fuera del rango.

Example Búsqueda del bloque de CIDR exacto 10.0.0.0/24

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Example Búsqueda de la dirección IP exacta 192.168.0.2/32

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

Comportamiento de múltiples propiedades en una matriz para consultas avanzadas

Al realizar la consulta de varias propiedades dentro de una matriz de objetos, las coincidencias se calculan para todos los elementos de la matriz.

Por ejemplo, para un recurso R con las reglas A y B, el recurso cumple con la regla A pero no cumple con la regla B. El recurso R se almacena como:

```
{
    configRuleList: [
```

```
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

R será devuelto por esta consulta:

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

La primera condición `configuration.configRuleList.complianceType = 'non_compliant'` se aplica a TODOS los elementos de R.configRuleList, dado que R tiene una regla (regla B) con ComplianceType = 'non_compliant', la condición se evalúa como verdadera.

La segunda condición `configuration.configRuleList.configRuleName` se aplica a TODOS los elementos de R.configRuleList, dado que R tiene una regla (regla A) con configRuleName = 'A', la condición se evalúa como verdadera. Como ambas condiciones son ciertas, se devolverá R.

Compatibilidad de la región

Las consultas avanzadas se admiten en las siguientes regiones:

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Este de EE. UU. (Norte de Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Oeste de EE. UU. (Norte de California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
África (Ciudad del Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Tailandia)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste de Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milán)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (España)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
México (centro)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Eliminar AWS Config datos

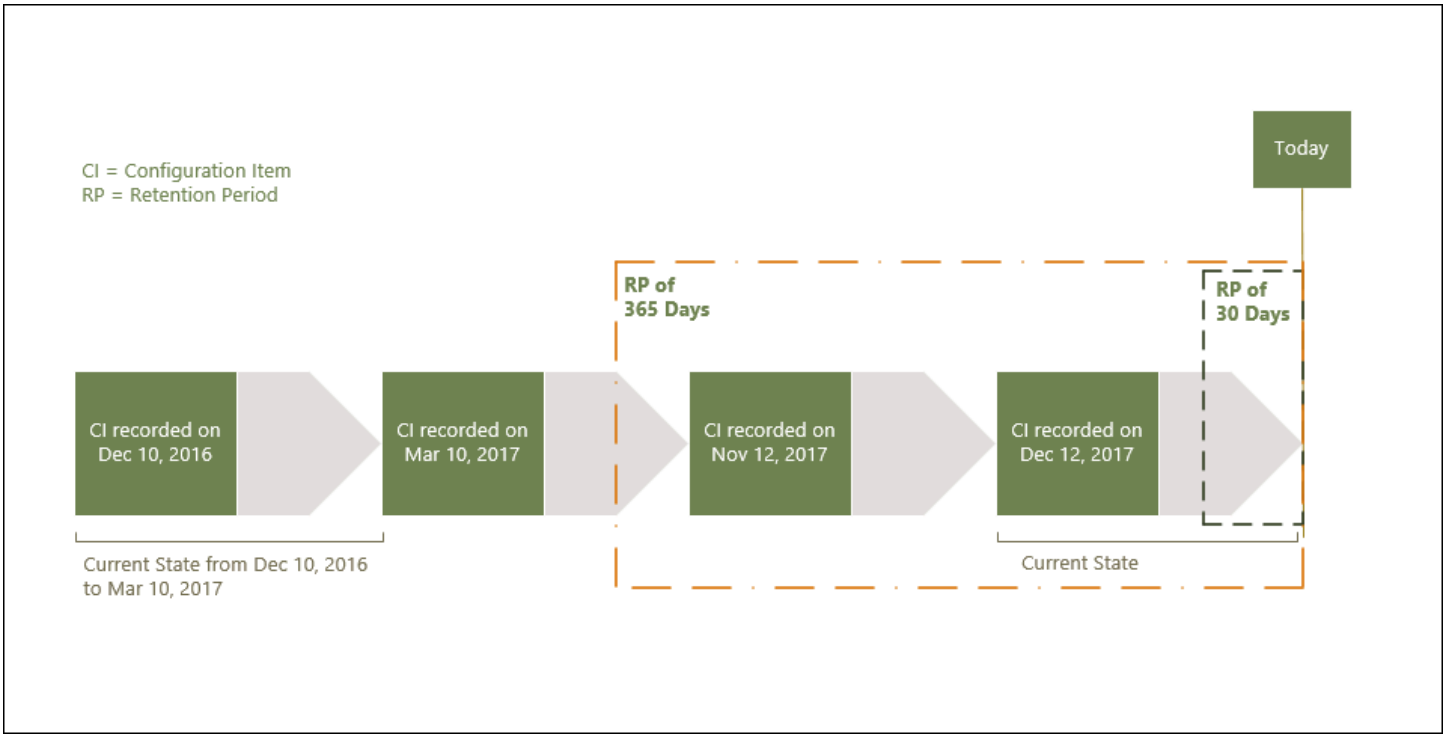
> **Note**
>
> Si bien AWS Config utiliza Amazon Simple Storage Service (Amazon S3) y Amazon Simple Notification Service (Amazon SNS) para enviar instantáneas de configuración y AWS Config archivos de historial de configuración, tiene sus propias políticas de almacenamiento y retención de datos. La información de esta página es específica para. AWS Config Amazon S3 y Amazon SNS tienen sus propias políticas de almacenamiento y retención de datos independientes.

AWS Config le permite eliminar sus datos especificando un período de retención para su`ConfigurationItems`. Cuando especificas un período de retención, lo AWS Config retiene `ConfigurationItems` durante ese período específico. Puede elegir un período entre un mínimo de 30 días y un máximo de 7 años (2557 días). AWS Config elimina los datos que tengan una antigüedad superior al período de retención especificado. Si no especifica un periodo de retención, AWS Config sigue almacenando `ConfigurationItems` durante el periodo predeterminado de 7 años (2557 días). Cuando el registro está activado, el estado actual del recurso es cuando se registra un `ConfigurationItem` y hasta que se registra el siguiente cambio (un `ConfigurationItem` nuevo).

Para comprender el comportamiento de periodo de retención, vamos a analizar la línea temporal.

- Cuando el registro está activado, el estado actual de un recurso siempre existe y no puede eliminarse independientemente de la fecha en que se registra el `ConfigurationItem`.
- Cuando AWS Config los registros son nuevos`ConfigurationItems`, los anteriores `ConfigurationItems` se eliminan en función del período de retención especificado.

En la siguiente escala de tiempo, AWS Config graba `ConfigurationItems` en las fechas siguientes. A efectos de esta línea temporal, hoy se representa como 24 de mayo de 2018.



En la siguiente tabla se explica qué `ConfigurationItems` se muestran en la línea temporal de AWS Config en función del periodo de retención seleccionado.

Periodo de retención	Elementos de configuración mostrados en la línea temporal	Explicación
30 días	12 de diciembre de 2017	El estado actual del recurso comenzó a partir del 12 de diciembre de 2017 cuando se registró el `ConfigurationItem` y es válido hasta hoy (24 de mayo de 2018). Cuando el registro está activado, el estado actual siempre existe.
365 días	12 de diciembre de 2017; 12 de noviembre de 2017 y 10 de marzo de 2017	El periodo de retención muestra el estado actual 12 de diciembre de 2017 y anteriores `ConfigurationItems` 12 de noviembre de 2017 y 10 de marzo de 2017.

Periodo de retención	Elementos de configuración mostrados en la línea temporal	Explicación
		El `ConfigurationItem` de 10 de marzo de 2017 se muestra en la escala de tiempo ya que ese estado de configuración representaba el estado actual hace 365 días.

Después de especificar un período de retención, ya AWS Config APIs no devolverá `ConfigurationItems` productos que representen un estado anterior al período de retención especificado.

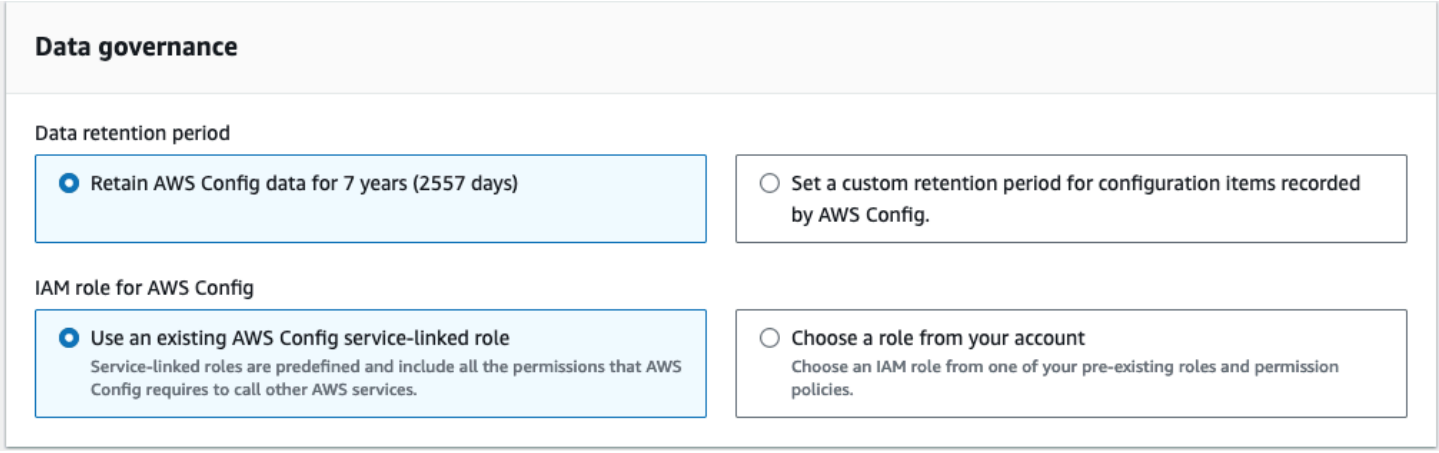
> **Note**
>
> - AWS Config no puede grabarlo `ConfigurationItems` si la grabación está desactivada.
> - AWS Config no puede grabarlo `ConfigurationItems` si su función de IAM no tiene permisos suficientes. Para obtener más información, consulte Permisos del rol de IAM asignado a. AWS Config

Establecer el período de retención de datos en Consola de administración de AWS

En el Consola de administración de AWS, si no selecciona un período de retención de datos, el período predeterminado es de 7 años o 2557 días.

Para establecer un periodo de retención de datos personalizado para elementos de configuración, seleccione la casilla de verificación. Puede seleccionar 1 año, 3 años, 5 años o un periodo preconfigurado. Para un periodo preconfigurado, escriba el número de días comprendido entre 30 y 2557 días.

En la siguiente imagen, se muestra dónde puede configurar el período de retención de datos en Gobernanza de datos. Para acceder a Data Governance en la página de edición de la configuración desde la AWS Config consola, seleccione Configuración en la barra de navegación izquierda y, a continuación, seleccione Editar.


Data governance
Data retention period
Retain AWS Config data for 7 years (2557 days)
Set a custom retention period for configuration items recorded by AWS Config.
IAM role for AWS Config
Use an existing AWS Config service-linked role
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.
Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.

Seguridad en AWS Config

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Config, consulte los AWS servicios de Scope by Compliance Program y .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Config. Los siguientes temas muestran cómo configurarlo AWS Config para cumplir sus objetivos de seguridad y conformidad.

Temas

- Protección de datos en AWS Config
- Identity and Access Management para AWS Config
- Respuesta a incidentes en AWS Config
- Validación de la conformidad para AWS Config
- Resiliencia en AWS Config
- Seguridad de la infraestructura en AWS Config
- Prevención de la sustitución confusa entre servicios
- Mejores prácticas de seguridad para AWS Config

Protección de datos en AWS Config

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Config. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contienen Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con AWS Config u otro tipo de Servicios de AWS uso de la consola AWS CLI, la API o AWS SDKs. Cualquier dato que introduzca

en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos en reposo

Los datos se cifran en reposo mediante cifrado transparente del lado del servidor. Esto ayuda a reducir la carga y la complejidad operativas que conlleva la protección de información confidencial. Con el cifrado en reposo, puede crear aplicaciones sensibles a la seguridad que cumplen los requisitos de cifrado y normativos.

Cifrado de datos en tránsito

Los datos recopilados y a los que se accede AWS Config se realizan exclusivamente a través de un canal protegido por Transport Layer Security (TLS).

Identity and Access Management para AWS Config

AWS Identity and Access Management (IAM) es un sistema Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Config La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración del acceso con políticas
- ¿Cómo AWS Config funciona con IAM
- Ejemplos de políticas basadas en la identidad para AWS Config
- AWS políticas gestionadas para AWS Config
- Permisos para el rol de IAM asignado a AWS Config
- Actualización del rol de IAM para el registrador de configuración administrado por el cliente
- Permisos del bucket de Amazon S3 para el canal AWS Config de entrega
- Permisos para la clave KMS del canal de AWS Config entrega

- Permisos para el tema de Amazon SNS
- Solución de problemas de AWS Config identidad y acceso
- Uso de funciones vinculadas a servicios para AWS Config

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Solución de problemas de AWS Config identidad y acceso).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte ¿Cómo AWS Config funciona con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Ejemplos de políticas basadas en la identidad para AWS Config).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas

políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Config funciona con IAM

Antes de utilizar IAM para gestionar el acceso AWS Config, infórmese sobre las funciones de IAM disponibles para su uso. AWS Config

Funciones de IAM que puede utilizar con AWS Config

Característica de IAM	AWS Config soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí

Característica de IAM	AWS Config soporte
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo AWS Config funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AWS Config

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para AWS Config

Para ver ejemplos de políticas AWS Config basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Config

Políticas basadas en recursos dentro de AWS Config

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para AWS Config

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de AWS Config acciones, consulte las acciones definidas AWS Config en la Referencia de autorización del servicio.

Las acciones políticas AWS Config utilizan el siguiente prefijo antes de la acción:

```
config
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "config:Describe*"
```

Para ver ejemplos de políticas AWS Config basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Config

Recursos de políticas para AWS Config

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de AWS Config recursos y sus tipos ARNs, consulte los recursos definidos AWS Config en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Config.

Para ver ejemplos de políticas AWS Config basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Config

Claves de condición de la política para AWS Config

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de AWS Config condición, consulte las claves de condición AWS Config en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Config.

Para ver ejemplos de políticas AWS Config basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Config

ACLs in AWS Config

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AWS Config

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Para obtener más información sobre el etiquetado de AWS Config recursos, consulte. Etiquetado de los recursos de AWS Config

Uso de credenciales temporales con AWS Config

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Sesiones de acceso directo para AWS Config

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama Servicio de AWS, junto con la solicitud, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Funciones de servicio para AWS Config

Compatible con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de AWS Config . Edite las funciones de servicio solo cuando se AWS Config proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AWS Config

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o la administración de funciones AWS Config vinculadas al servicio, consulte. Uso de funciones vinculadas a servicios para AWS Config

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para AWS Config

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de AWS Config . Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos ARNs por AWS Config cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de AWS Config la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Inscríbase en una Cuenta de AWS
- Creación de un usuario con acceso administrativo
- Uso de la consola AWS Config
- Cómo permitir a los usuarios consultar sus propios permisos
- Acceso de solo lectura a AWS Config
- Acceso completo a AWS Config

- Permisos a nivel de recursos compatibles para las acciones de la API de AWS Config reglas
- Permisos de nivel de recursos para la agregación de datos de varias regiones y varias cuentas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS Config recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar Tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puedes ver la actividad de tu cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión Consola de administración de AWScomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Uso de la consola AWS Config

Para acceder a la AWS Config consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS Config recursos de su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la AWS Config consola, adjunte también la política AWS Config `AWSConfigUserAccess` AWS administrada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Debe conceder a los usuarios permisos para interactuar con ellas AWS Config. Para los usuarios que necesitan acceso total a ella AWS Config, utilice la política de acceso total a la AWS Config gestión.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .
- Usuarios gestionados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:

- Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
- (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Acceso de solo lectura a AWS Config

El siguiente ejemplo muestra una política AWS administrada `AWSConfigUserAccess` que concede acceso de solo lectura a. AWS Config

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

En las declaraciones de políticas, el elemento `Effect` especifica si las acciones se permiten o se niegan. El elemento `Action` enumera las acciones específicas que puede realizar el usuario. El `Resource` elemento enumera los AWS recursos en los que el usuario puede realizar esas acciones. En el caso de las políticas que controlan el acceso a AWS Config las acciones, el `Resource` elemento siempre está configurado como`*`, un comodín, que significa «todos los recursos».

Los valores del `Action` elemento corresponden a los APIs que admiten los servicios. Las acciones van precedidas de `config:` para indicar que se refieren a AWS Config acciones. Puede utilizar el carácter comodín `*` en el elemento `Action`, como en los siguientes ejemplos:

- `"Action": ["config:*ConfigurationRecorder"]`

  Esto permite todas AWS Config las acciones que terminan en "ConfigurationRecorder" (`StartConfigurationRecorder`,`StopConfigurationRecorder`).
- `"Action": ["config:*"]`

  Esto permite todas AWS Config las acciones, pero no las acciones de otros AWS servicios.
- `"Action": ["*"]`

  Esto permite todas AWS las acciones. Este permiso es adecuado para un usuario que actúa como AWS administrador de su cuenta.

La política de solo lectura no concede permiso al usuario para acciones como `StartConfigurationRecorder`, `StopConfigurationRecorder` y `DeleteConfigurationRecorder`. Los usuarios con esta política no pueden comenzar un registro de configuración, detener un registro de configuración o eliminar un registro de configuración. Para ver la lista de AWS Config acciones, consulta la referencia de la AWS Config API.

Acceso completo a AWS Config

El siguiente ejemplo muestra una política que concede acceso total a AWS Config. Concede a los usuarios el permiso para realizar todas AWS Config las acciones. También permite a los usuarios administrar archivos en buckets de Amazon S3 y administrar los temas de Amazon SNS en la cuenta a la que está asociado el usuario.

> **Important**
>
> Esta política otorga amplios permisos. Antes de otorgar acceso total, es recomendable empezar con un conjunto mínimo de permisos y otorgar permisos adicionales según sea necesario. Por lo general, es más seguro que comenzar con permisos que son demasiado tolerantes y querer restringirlos más adelante.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
```

```
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

Permisos a nivel de recursos compatibles para las acciones de la API de AWS Config reglas

Los permisos a nivel de recursos se refieren a la capacidad de especificar en qué recursos los usuarios pueden realizar acciones. AWS Config admite permisos a nivel de recurso para determinadas acciones de la API de reglas AWS Config . Esto significa que, para determinadas acciones de AWS Config reglas, puedes controlar las condiciones en las que los usuarios pueden usar esas acciones. Estas condiciones pueden ser acciones que se deben cumplir o recursos específicos que los usuarios pueden utilizar.

En la siguiente tabla se describen las acciones de la API de AWS Config reglas que actualmente admiten permisos a nivel de recurso. También se describen los recursos admitidos y los ARNs correspondientes a cada acción. Al especificar un ARN, puede usar el comodín * en sus rutas; por ejemplo, cuando no puede o no quiere especificar el recurso exacto. IDs

> **Important**
>
> Si una acción de la API de una AWS Config regla no aparece en esta tabla, significa que no admite permisos a nivel de recurso. Si una acción de AWS Config regla no admite permisos a nivel de recursos, puedes conceder permisos a los usuarios para que usen la acción, pero tendrás que especificar un asterisco (*) para el elemento de recurso de tu declaración de política.

Acción API	Recursos
DeleteConfigRule	Regla de configuración arn:aws:config ::config-rule/config-rule- *region:accountID ID*
DeleteEvaluationResults	Regla de configuración arn:aws:config ::config-rule/config-rule *region:accountID* - *ID*
DescribeCompliance ByConfigRule	Regla de configuración arn:aws:config ::config-rule/config-rule *region:accountID* - *ID*
DescribeConfigRuleEvaluatio nStatus	Regla de configuración arn:aws:config ::config-rule/config-rule *region:accountID* - *ID*
GetComplianceDetailsByConfi gRule	Regla de configuración arn:aws:config ::config-rule/config-rule *region:accountID* - *ID*
PutConfigRule	Regla de configuración arn:aws:config ::config-rule/config-rule *region:accountID* - *ID*
StartConfigRulesEvaluation	Regla de configuración arn:aws:config ::config-rule/config-rule *region:accountID* - *ID*
PutRemediationConfigurations	Configuración de la corrección

Acción API	Recursos
	arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DescribeRemediationConfigurations	Configuración de la corrección arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DeleteRemediationConfiguration	Configuración de la corrección arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
PutRemediationExceptions	Configuración de la corrección arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DescribeRemediationExceptions	Configuración de la corrección arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DeleteRemediationExceptions	Configuración de la corrección arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*

Por ejemplo, desea permitir a usuarios específicos el acceso de lectura y denegar el acceso de escritura a reglas específicas.

En la primera política, se permite que la regla lea acciones como, por ejemplo, en las reglas especificadas AWS Config . `DescribeConfigRuleEvaluationStatus`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "config:StartConfigRulesEvaluation",
                "config:DescribeComplianceByConfigRule",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": [
                "arn:aws:config:us-east-1:123456789012:config-rule/config-
rule-ID",
                "arn:aws:config:us-east-1:123456789012:config-rule/config-
rule-ID"
            ]
        }
    ]
}
```

En la segunda política, deniegas a la AWS Config regla la escritura de acciones en la regla específica.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
```

```
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
            ],
            "Resource": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-ID"
        }
    ]
}
```

Con los permisos a nivel de recursos, puedes permitir el acceso de lectura y denegar el acceso de escritura para realizar acciones específicas en las acciones de la API de AWS Config reglas.

Permisos de nivel de recursos para la agregación de datos de varias regiones y varias cuentas

Puede utilizar los permisos de nivel de recursos para controlar la capacidad de un usuario de realizar acciones específicas en la acumulación de datos de varias cuentas y regiones. Los siguientes permisos de nivel de recurso AWS Config `Aggregator` APIs admiten:

- BatchGetAggregateResourceConfig
- DeleteConfigurationAggregator
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStatus
- GetAggregateComplianceDetailsByConfigRule
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceCounts
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAggregator
- SelectAggregateResourceConfig

Por ejemplo, puede restringir el acceso de usuarios específicos a los datos de los recursos mediante la creación de los dos agregadores `AccessibleAggregator` y `InAccessibleAggregator` y

asociar una política de IAM que permita el acceso a `AccessibleAggregator` pero deniegue el acceso a `InAccessibleAggregator`.

Política de IAM para AccessibleAggregator

En esta política, permite el acceso a las acciones del agregador compatibles con el nombre de recurso de Amazon (ARN) de AWS Config que especifique. En este ejemplo, el AWS Config ARN es. `arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:111122223333:config-
aggregator/config-aggregator-mocpsqhs"
        }
    ]
}
```

Política de IAM para InAccessibleAggregator

En esta política, deniega el acceso a las acciones del agregador compatibles con el ARN de AWS Config que especifique. En este ejemplo, el AWS Config ARN es. `arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:111122223333:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
}
```

Si un usuario del grupo de desarrolladores intenta realizar alguna de estas acciones en el ARN de AWS Config que especificó, ese usuario recibirá una excepción de acceso denegado.

Comprobar los permisos de acceso de los usuarios

Para mostrar los agregadores que ha creado, ejecute el siguiente comando de la AWS CLI :

```
aws configservice describe-configuration-aggregators
```

Cuando el comando se haya completado correctamente, podrá ver los detalles de todos los agregadores asociados a su cuenta. En este ejemplo, se trata de `AccessibleAggregator` y `InAccessibleAggregator`:

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
```

```
    ]
}
```

> **Note**
>
> Para `account-aggregation-sources` introducir una lista separada por comas de las AWS cuentas IDs para las que desee agregar datos. Coloque la cuenta IDs entre corchetes y asegúrese de evitar las comillas (por ejemplo,`"[{\"AccountIds\": [\"AccountID1\", \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).

Asocie la siguiente política de IAM para denegar el acceso a `InAccessibleAggregator` o el agregador al que desea denegar el acceso.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:111122223333:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
```

```
}
```

A continuación, puede confirmar que la política de IAM funciona para restringir el acceso a las reglas al agregador específico.

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

El comando debería devolver una excepción de acceso denegado:

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

AWS políticas gestionadas para AWS Config

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSConfigServiceRolePolicy

AWS Config utiliza el rol vinculado al servicio denominado AWSServiceRoleForConfigpara llamar a otros AWS servicios en su nombre. Al utilizar el Consola de administración de AWS para configurarlo AWS Config, esta SLR se crea automáticamente AWS Config si selecciona la opción de utilizar la AWS Config SLR en lugar de su propia función de servicio AWS Identity and Access Management (IAM).

El SLR AWSServiceRoleForConfig contiene la política administrada `AWSConfigServiceRolePolicy`. Esta política gestionada contiene permisos de solo lectura y solo escritura para los recursos y permisos de solo lectura para AWS Config los recursos de otros servicios compatibles. AWS Config La política proporciona un acceso integral para monitorear y registrar los cambios de configuración en toda la AWS infraestructura, incluidos los permisos para más de 100 AWS servicios, como los servicios de computación, almacenamiento, redes, seguridad, análisis y aprendizaje automático.

La política incluye permisos para las siguientes categorías de servicios:

- `access-analyzer`— Permite a los directores analizar los patrones de acceso y recuperar los hallazgos de seguridad.
- `account`— Permite a los directores recuperar la información de contacto de la cuenta.
- `acm`y `acm-pca` — Permite a los directores gestionar los SSL/TLS certificados y las autoridades de certificación privadas.
- `airflow`— Permite a los directores monitorear los entornos gestionados de Apache Airflow.
- `amplify`y `amplifyuibuilder` — Permite a los directores monitorear las aplicaciones web y los componentes de la interfaz de usuario.
- `aoss`— Permite a los directores monitorear las colecciones OpenSearch sin servidor y las configuraciones de seguridad.
- `app-integrations`— Permite a los directores monitorear las configuraciones de integración de las aplicaciones.
- `appconfig`— Permite a los directores monitorear las implementaciones de configuración de las aplicaciones.
- `appflow`— Permite a los directores monitorear las configuraciones del flujo de datos entre aplicaciones.
- `application-autoscaling`y`application-signals`: permite a los directores monitorear las políticas de autoscalamiento y las métricas de rendimiento de las aplicaciones.

- `appmesh`— Permite a los directores monitorear las configuraciones de la malla de servicios.
- `apprunner`— Permite a los directores monitorear las aplicaciones y servicios web en contenedores.
- `appstream`— Permite a los directores monitorear las configuraciones de transmisión de aplicaciones.
- `appsync`— Permite a los directores supervisar las configuraciones de la API de GraphQL.
- `aps`— Permite a los directores monitorear las configuraciones de monitoreo de Prometheus.
- `apptest`— Permite a los directores monitorear las configuraciones de las pruebas de las aplicaciones.
- `arc-zonal-shift`— Permite a los directores monitorear la disponibilidad de las configuraciones de los cambios zonales.
- `athena`— Permite a los directores monitorear las configuraciones de los motores de consultas y los catálogos de datos.
- `auditmanager`— Permite a los directores supervisar las evaluaciones de auditoría y cumplimiento.
- `autoscaling`y `autoscaling-plans` — Permite a los directores monitorear los grupos de autoescalado y los planes de escalado.
- `b2bi`— Permite a los directores monitorear business-to-business las configuraciones de integración.
- `backup`y `backup-gateway` — Permite a los directores monitorear las políticas de respaldo y las configuraciones de las puertas de enlace.
- `batch`— Permite a los directores monitorear los entornos de computación por lotes y las colas de trabajos.
- `bcm-data-exports`— Permite a los directores monitorear las exportaciones de datos de facturación y gestión de costos.
- `bedrock`y `bedrock-agentcore` — Permite a los directores monitorear los modelos básicos y las configuraciones de los agentes de IA.
- `billingconductor`— Permite a los directores supervisar las configuraciones de los grupos de facturación.
- `budgets`— Permite a los directores monitorear las configuraciones y acciones del presupuesto.
- `cassandra`— Permite a los directores consultar las configuraciones de las bases de datos gestionadas de Cassandra.
- `ce`— Permite a los directores monitorear las configuraciones de los informes de costos y uso.

- `cleanroomsy cleanrooms-ml` — Permite a los directores monitorear las configuraciones de colaboración de datos y aprendizaje automático.
- `cloud9`— Permite a los directores monitorear las configuraciones del entorno de desarrollo en la nube.
- `cloudformation`— Permite a los directores monitorear la infraestructura como configuraciones de pila de códigos.
- `cloudfront`— Permite a los directores monitorear las configuraciones de la red de entrega de contenido.
- `cloudtrail`— Permite a los directores monitorear las configuraciones de registro de API y registros de auditoría.
- `cloudwatch`— Permite a los directores monitorear las métricas, las alarmas y las configuraciones del panel de control.
- `codeartifact`— Permite a los directores monitorear las configuraciones de los repositorios de paquetes de software.
- `codebuild`— Permite a los directores monitorear las configuraciones del proyecto de construcción.
- `codecommit`— Permite a los directores monitorear las configuraciones del repositorio de código fuente.
- `codeconnections`— Permite a los directores monitorear las conexiones de fuentes de terceros.
- `codedeploy`— Permite a los directores monitorear las configuraciones de implementación de las aplicaciones.
- `codeguru-profilery codeguru-reviewer` — Permite a los directores monitorear las configuraciones de análisis de código y creación de perfiles.
- `codepipeline`— Permite a los directores monitorear las configuraciones continuas de los procesos de integración y despliegue.
- `codestar-connections`— Permite a los directores monitorear las conexiones entre las herramientas de los desarrolladores.
- `cognito-identityy cognito-idp` — Permite a los directores monitorear la identidad y las configuraciones del grupo de usuarios.
- `comprehend`— Permite a los directores monitorear las configuraciones de procesamiento del lenguaje natural.
- `config`— Permite a los directores gestionar el registro de la configuración y la supervisión del cumplimiento.

- `connect`— Permite a los directores monitorear las configuraciones del centro de contacto.

Para obtener más información sobre los tipos de recursos compatibles, consulte Tipos de recursos compatibles para AWS Config yUso de funciones vinculadas a servicios para AWS Config.

Para ver más detalles sobre la política, incluyendo la última versión del documento de política JSON, consulte AWSConfigServiceRolePolicy en la Guía de referencia de políticas administradas de AWS .

> **Recomendación: Utilice el rol vinculado al servicio**
>
> Es recomendable utilizar el rol vinculado a servicios a menos que tenga un caso de uso concreto. Un rol vinculado a un servicio añade todos los permisos necesarios para que AWS Config se ejecute según lo esperado. Algunas características, como los registradores de configuración vinculados con servicios, requieren el uso del rol vinculado a servicios.

AWS política gestionada: AWS_ConfigRole

Para registrar las configuraciones AWS de sus recursos, AWS Config necesita permisos de IAM para obtener los detalles de configuración de sus recursos. Si desea crear un rol de IAM para AWS Config, puede utilizar la política administrada `AWS_ConfigRole` y asociarla a su rol de IAM.

Esta política de IAM se actualiza cada vez que AWS Config añade compatibilidad con un tipo de AWS recurso. Esto significa que AWS Config seguirá teniendo los permisos necesarios para registrar los datos de configuración de los tipos de recursos compatibles siempre que la función AWS_COnFigrole tenga asociada esta política gestionada. La política proporciona un acceso integral para monitorear y registrar los cambios de configuración en toda la AWS infraestructura, incluidos los permisos para más de 100 AWS servicios, como los servicios de computación, almacenamiento, redes, seguridad, análisis y aprendizaje automático. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config y Permisos para el rol de IAM asignado a AWS Config.

Para ver más detalles sobre la política, incluida la última versión del documento de política de JSON, consulte AWS_COnFigrole en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: AWSConfigUserAccess

Esta política de IAM proporciona acceso al uso AWS Config, incluida la búsqueda por etiquetas en los recursos y la lectura de todas las etiquetas. Esto no proporciona permiso de configuración AWS Config, lo que requiere privilegios administrativos.

Consulte la política: AWSConfigUserAccess.

AWS política gestionada: ConfigConformsServiceRolePolicy

Para implementar y administrar los paquetes de conformidad, se AWS Config requieren permisos de IAM y ciertos permisos de otros AWS servicios. Estos le permiten implementar y gestionar los paquetes de conformidad con todas las funciones y se actualizan cada vez que se AWS Config añaden nuevas funciones a los paquetes de conformidad. Para obtener más información sobre los paquetes de conformidad, consulte Paquetes de conformidad.

Consulte la política: ConfigConformsServiceRolePolicy.

AWS política gestionada: AWSConfigRulesExecutionRole

Para implementar reglas Lambda AWS personalizadas, se AWS Config requieren permisos de IAM y ciertos permisos de otros servicios. AWS Permiten que AWS Lambda las funciones accedan a la AWS Config API y a las instantáneas de configuración que AWS Config se envían periódicamente a Amazon S3. Este acceso lo requieren las funciones que evalúan los cambios de configuración de las reglas Lambda AWS personalizadas y se actualiza cada vez que se AWS Config agrega una nueva funcionalidad. Para obtener más información sobre las reglas Lambda AWS personalizadas, consulte Creación de reglas AWS Config Lambda personalizadas. Para obtener más información sobre las instantáneas de configuración, consulte Conceptos | Instantánea de configuración. Para obtener más información sobre la entrega de instantáneas de configuración, consulte Administrar el canal de entrega.

Consulte la política: AWSConfigRulesExecutionRole.

AWS política gestionada: AWSConfigMultiAccountSetupPolicy

Para implementar, actualizar y eliminar de forma centralizada AWS Config las reglas y los paquetes de conformidad en las cuentas de los miembros de una organización AWS Organizations, se AWS Config requieren permisos de IAM y ciertos permisos de otros AWS servicios. Esta política administrada se actualiza cada vez que AWS Config añade nuevas funciones a la configuración de varias cuentas. Para obtener más información, consulte Administrar AWS Config las reglas en todas las cuentas de su organización y Administrar los paquetes de conformidad en todas las cuentas de su organización.

Consulte la política: AWSConfigMultiAccountSetupPolicy.

AWS política gestionada: AWSConfigRoleForOrganizations

AWS Config Para permitir las llamadas de solo lectura AWS Organizations APIs, AWS Config requiere permisos de IAM y algunos permisos de otros servicios. AWS Esta política administrada se actualiza cada vez que AWS Config añade nuevas funciones a la configuración de varias cuentas. Para obtener más información, consulte Administrar AWS Config las reglas en todas las cuentas de su organización y Administrar los paquetes de conformidad en todas las cuentas de su organización.

Consulte la política: AWSConfigRoleForOrganizations.

AWS política gestionada: AWSConfigRemediationServiceRolePolicy

Para poder AWS Config corregir `NON_COMPLIANT` los recursos en su nombre, AWS Config requiere permisos de IAM y ciertos permisos de otros AWS servicios. Esta política gestionada se actualiza cada vez que se AWS Config añade una nueva funcionalidad de corrección. Para obtener más información sobre la corrección, consulte Remediar recursos no conformes con reglas. AWS Config Para obtener más información sobre las condiciones que originan los posibles resultados de la AWS Config evaluación, consulte Conceptos | Reglas. AWS Config

Consulte la política: AWSConfigRemediationServiceRolePolicy.

AWS Config actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Config desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS Config documento.

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy— Política gestionada actualizada con permisos integrales para el registro de la configuración de los AWS recursos en más de 100 AWS servicios, incluidos los servicios de computación, almacenam	Esta política ahora proporciona una documentación mejorada de los permisos de los servicios y permite una supervisión integral de todos los AWS servicios que AWS Config permiten el registro de la configuración.	27 de enero de 2026

Cambio	Descripción	Fecha
iento, redes, seguridad , análisis y aprendizaje automático.		
AWS_ConfigRole— Política gestionada actualizada con permisos integrales para el registro de la configura ción de AWS recursos en más de 100 AWS servicios , incluidos los servicios de computación, almacenam iento, redes, seguridad , análisis y aprendizaje automático.	Esta política ahora proporcio na una documentación mejorada de los permisos de los servicios y permite una supervisión integral de todos los AWS servicios que AWS Config permiten el registro de la configuración.	27 de enero de 2026
AWS_ConfigRole— añadir «s3tables: ListTagsF orResource «, «s3tables:», «s3tables:GetTableBucketMet ricsConfiguration» GetTableB ucketStorageClass	Esta política ahora admite permisos adicionales para S3Tables.	09 de enero de 2026
AWSConfigServiceRo lePolicy— añadir «s3tables : ListTagsForResource «, «s3tables:», «s3tables :GetTableBucketMetricsConfi guration» GetTableBucketStor ageClass	Esta política ahora admite permisos adicionales para S3Tables.	09 de enero de 2026
AWS_ConfigRole— añadir «lightsailGetActiveNames»: «lightsail»: «s3:GetOp erations» GetBucketAbac	Esta política ahora admite permisos adicionales para Amazon Lightsail y Amazon Simple Storage Service (Amazon S3).	20 de noviembre de 2025

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy— añadir «lightsailGetActiveNames»: «lightsail»: «s3:GetOperations» GetBucketAbac	Esta política ahora admite permisos adicionales para Amazon Lightsail y Amazon Simple Storage Service (Amazon S3).	20 de noviembre de 2025
AWSConfigServiceRolePolicy— Política gestionada actualizada con permisos integrales para el registro de la configuración de AWS recursos en más de 100 AWS servicios, incluidos los servicios de computación, almacenamiento, redes, seguridad, análisis y aprendizaje automático.	Esta política ahora proporciona una documentación mejorada de los permisos de los servicios y permite una supervisión integral de todos los AWS servicios que AWS Config permiten el registro de la configuración.	11 de noviembre de 2025
AWS_ConfigRole— Política gestionada actualizada con permisos integrales para el registro de la configuración de AWS recursos en varios servicios AWS Identity and Access Management, incluidos Amazon Elastic Compute Cloud, Amazon Simple Storage Service y Amazon Relational Database Service y muchos otros. AWS Lambda	Esta política ahora admite permisos adicionales para la configuración, el registro y la supervisión integrales de los AWS recursos en todos los AWS servicios compatibles.	10 de noviembre de 2025

Cambio	Descripción	Fecha
AWS_ConfigRole— añadir «amplify:GetDomainAssociation» «amplify:ListDomainAssociations» «appsync: ListTagsForResource» appsync: GetSourceApiAssociation «bedrock:ListSourceApiAssociations» bedrock: GetFlow «bedrock:ListAgentCollaborators» bedrock: «cloudTrail:ListFlows» cloudformation:ListPrompts» codeartifact: GetResourcePolicy «codeartifact:DescribePublisher» codeartifact: DescribePackageGroup «codeartifact:ListAllowedRepositoriesForGroup" «codepipeline:ListPackageGroups" «codepipeline:ListActionTypes" «codepipeline:ListTagsForResource" «connect:ListWebhooks" connect: DescribeTrafficDistributionGroup "«fecha límite:ListTrafficDistributionGroups" «ec2:ListFarms" «ec2:GetTransitGatewayRouteTablePropagations» ec2: SearchLocalGatewayRoutes SearchTransitGatewayMulticastGroups« entityresolution:GetMatchingWorkflow" «entityresolution:ListMatchingWorkfl	Esta política ahora admite permisos adicionales para AWS Amplify AWS AppSync, Amazon Bedrock,, AWS CloudTrail, CloudFormation AWS CodeArtifact, Amazon Connect AWS CodePipeline, Amazon EC2 AWS Deadline Cloud,, Amazon IVS AWS Entity Resolution AWS IoT SiteWise, Amazon, Amazon Quick AWS Lambda EventBridge, Amazon Redshift, Amazon Redshift Serverless AWS Identity and Access Management Roles Anywhere, Amazon, Amazon Security Lake AWS Service Catalog, SageMaker AWS Secrets Manager AWS Shield Amazon EC2 Systems Manager y. AWS WAFV2	1 de octubre de 2025

Cambio	Descripción	Fecha
ows" «iotsitewise:ListA ssetModelCompositeModels" «iotsitewise:ListAssetModel Properties" «iotsitewise:ListA ssetProperties" «iotsitewise: ListAssociatedAssetsListPub licKeys" «ivs:GetProvisione dConcurrencyConfig» lambda: GetRuntimeManageme ntConfig «lambda:ListFuncti onEventInvokeConfigs» lambda: «lambda:ListFuncti onUrlConfigs» «pipes:De scribePipe» «pipes:ListPipes» quicksight: DescribeR efreshSchedule «redshift- serverless:ListSnapshotCop yConfigurations" «shift: «roles en cualquier lugar:Get ResourcePolicy» «roles en cualquier lugar:Lis tCrls» «sagemaker:Describ eApp» «sagemaker:Describ eUserProfile» «sagemaker: ListRefreshSchedules GetCrl ListApps««sagemaker:ListMod elPackages» «sagemake r:ListUserProfiles» «secretsm anager:GetResourcePolicy» «securitylake:ListSubscribers» «securitylake:ListTagsForRe source» «catálogo de servicios:DescribeServiceAc tion» «catálogo de servicios :ListApplications» «escudo:»		

Cambio	Descripción	Fecha
«ssm-incidentes:ListAssociatedResources» «ssm-incidentes:ListTagsForResource» «ssm:GetReplicationSet» «ssm:» «ssm:ListReplicationSets» «ssm:DescribeAssociation» «ssm:DescribePatchBaselines» ssm: GetDefaultPatchBaseline «ssm:GetPatchBaseline» ssm: GetResourcePolicies «ssm:ListAssociations» sm: "«ssm:ListResourceDataSync" «wafv2:ListLoggingConfigurations" «bedrock-agentcore:ListCodeInterpreters" «bedrock-agentcore:GetCodeInterpreter» bedrock ListProtectionGroups - núcleo de agente: ListBrowsers «núcleo de agente de roca madre:GetBrowser» «núcleo de agente de roca madre: ListAgentRuntimesGetAgentRuntime» «núcleo de agente de roca madre:» ListAgentRuntimeEndpoints «núcleo de agente de roca madre:GetAgentRuntimeEndpoint»		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy— añadir «amplify: GetDomainAssociation» «amplify:ListDomainAssociations» «appsync:ListTagsForResource» appsync: GetSourceApiAssociation «bedrock:ListSourceApiAssociations» bedrock: GetFlow «bedrock:ListAgentCollaborators» bedrock: ListFlows «cloudTrail:ListPrompts» cloudformation:GetResourcePolicy» codeartifact: DescribePublisher «codeartifact:DescribePackageGroup» codeartifact: ListAllowedRepositoriesForGroup «codeartifact:ListPackageGroups" «codepipeline:ListActionTypes" «codepipeline:ListTagsForResource" «codepipeline:ListWebhooks" «connect: DescribeTrafficDistributionGroup" connect: ListTrafficDistributionGroups "«fecha límite:ListFarms" «ec2:GetTransitGatewayRouteTablePropagations" «ec2:SearchLocalGatewayRoutes» ec2: SearchTransitGatewayMulticastGroups«entityresolution:GetMatchingWorkflow" «entityresolution:ListMatchingWorkfl	Esta política ahora admite permisos adicionales para AWS Amplify AWS AppSync, Amazon Bedrock,, AWS CloudTrail, CloudFormation AWS CodeArtifact, Amazon Connect AWS CodePipeline, Amazon EC2 AWS Deadline Cloud,, Amazon IVS AWS Entity Resolution AWS IoT SiteWise, Amazon, Amazon Quick AWS Lambda EventBridge, Amazon Redshift, Amazon Redshift Serverless AWS Identity and Access Management Roles Anywhere, Amazon, Amazon Security Lake AWS Service Catalog, SageMaker AWS Secrets Manager AWS Shield Amazon EC2 Systems Manager y. AWS WAFV2	1 de octubre de 2025

Cambio	Descripción	Fecha
ows" «iotsitewise:ListA ssetModelCompositeModels" «iotsitewise:ListAssetModel Properties" «iotsitewise:ListA ssetProperties" «iotsitewise: ListAssociatedAssetsListPub licKeys" «ivs:GetProvisione dConcurrencyConfig» lambda: GetRuntimeManageme ntConfig «lambda:ListFuncti onEventInvokeConfigs» lambda: «lambda:ListFuncti onUrlConfigs» «pipes:De scribePipe» «pipes:ListPipes» quicksight: DescribeR efreshSchedule «redshift- serverless:ListSnapshotCop yConfigurations" «shift: «roles en cualquier lugar:Get ResourcePolicy» «roles en cualquier lugar:Lis tCrls» «sagemaker:Describ eApp» «sagemaker:Describ eUserProfile» «sagemaker: ListRefreshSchedules GetCrl ListApps««sagemaker:ListMod elPackages» «sagemake r:ListUserProfiles» «secretsm anager:GetResourcePolicy» «securitylake:ListSubscribers» «securitylake:ListTagsForRe source» «catálogo de servicios:DescribeServiceAc tion» «catálogo de servicios :ListApplications» «escudo:»		

Cambio	Descripción	Fecha
«ssm-incidentes:ListAssociatedResources» «ssm-incidentes:ListTagsForResource» «ssm:GetReplicationSet» «ssm:» «ssm:ListReplicationSets» «ssm:DescribeAssociation» «ssm:DescribePatchBaselines» ssm: GetDefaultPatchBaseline «ssm:GetPatchBaseline» ssm: GetResourcePolicies «ssm:ListAssociations» sm: "«ssm:ListResourceDataSync" «wafv2:ListLoggingConfigurations" «bedrock-agentcore:ListCodeInterpreters" «bedrock-agentcore:GetCodeInterpreter» bedrock ListProtectionGroups - núcleo de agente: ListBrowsers «núcleo de agente de roca madre:GetBrowser» «núcleo de agente de roca madre: ListAgentRuntimesGetAgentRuntime» «núcleo de agente de roca madre:» ListAgentRuntimeEndpoints «núcleo de agente de roca madre:GetAgentRuntimeEndpoint»		

Cambio	Descripción	Fecha
AWS_ConfigRole— Añade «arc-zonal-shift: GetAutoshiftObserverNotificationStatus «, «bedrock: GetModelInvocationLoggingConfiguration «, «cloudtrail: GetEventConfiguration «, «codeartifact: DescribeDomain «, GetDomainPermissionsPolicy «codeartifact: «, GetFleet «deadline: GetQueueFleetAssociation «, «deadline: ListFleets «, «deadline: ListQueueFleetAssociations «, «deadline: ListTagsForResource «, «dms: DescribeDataMigrations «, «dms: ListMigrationProjects «, GetDataCatalogEncryptionSettings «glue: «, «kafkaconnect: DescribeCustomPlugin «, DescribeWorkerConfiguration «kafkaconnect: «, ListCustomPlugins «kafkaconnect: «, ListTagsForResource «kafkaconnect: ListWorkerConfigurations «, «lake formation: DescribeLakeFormationIdentityCenterConfiguration «, «medialive: DescribeMultiplexProgram «, «medialive: ListMultiplexPrograms«, «mediapackage v2: GetChannelGroup «,	Esta política ahora admite permisos adicionales para Amazon Bedrock AWS ARC - Zonal Shift,,,, AWS CloudTrail, AWS CodeArtifact AWS Deadline Cloud AWS Database Migration Service AWS Glue AWS Identity and Access Management, Amazon Managed Streaming for Apache Kafka Kafka AWS Lake Formation, CloudWatch Amazon Logs AWS Elemental MediaLive, AWS Elemental MediaPackage, Amazon Relational Database Service, Amazon Simple Storage Service AWS Secrets Manager, Amazon Security Lake AWS Service Catalog, Amazon Simple Email Service y. AWS X-Ray	28 de julio de 2025

Cambio	Descripción	Fecha
«mediapackage v2: ListChannelGroups «, «rds: «, DescribeEngineDefaultParameters «roles en cualquier parte: GetProfile «, «roles en cualquier parte: GetTrustAnchor «, «roles en cualquier parte: ListProfiles «, «roles en cualquier parte: ListTagsForResource «, «s3: ListTrustAnchors «, «s3: GetAccessGrant «, «administrador de secretos: ListAccessGrants «, «security lake: DescribeSecret «, «security lake: ListDataLakeExceptions «, «security lake: ListDataLakes «, «security lake: ListLogSources «, «security lake: GetAttributeGroup «: «, «catálogo de servicios: ListAttributeGroups «, «catálogo de servicios: ListServiceActions «, «catálogo de servicios: ListServiceActionsForProvisioningArtifact «, «catálogo de servicios: GetTrafficPolicy «, «ses: ListTagsForResource «,» ver: ListTrafficPolicies «, «radiografía: GetGroup «, GetGroups «radiografía: «, GetSamplingRules «radiografía: ListResourcePolicies «,		

Cambio	Descripción	Fecha
«radiografía:ListTagsForResource»		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy – Add "arc-zonal-shift: GetAutoshiftObserverNotificationStatus «, «bedrock: «, «cloudtrail: GetModelInvocationLoggingConfiguration «, «codeartifact: GetEventConfiguration «, «codeartifact: «, «deadline: DescribeDomain «, «deadline: «, «deadline: «, «deadline: GetDomainPermissionsPolicy «, «deadline: «, GetFleet «dms: «, «dms: GetQueueFleetAssociation «, «glue: «, ListFleets «iam: «, «kafkaconnect: ListQueueFleetAssociations «, kafkaconnect: ListTagsForResource «, kafkaconnect: «, kafkaconnect: DescribeDataMigrations «, kafkaconnect: ListMigrationProjects «, kafkaconnect: «, kafkaconnect: GetDataCatalogEncryptionSettings «, kafkaconnect: «, kafkaconnect: ListPolicies «, kafkaconnect: DescribeCustomPlugin «, kafkaconnect: «, kafkaconnect: DescribeWorkerConfiguration «, kafkaconnect: «, kafkaconnect: ListCustomPlugins «, kafkaconnect:	Esta política ahora admite permisos adicionales para Amazon Bedrock AWS ARC - Zonal Shift,,,, AWS CloudTrail, AWS CodeArtifact AWS Deadline Cloud AWS Database Migration Service AWS Glue AWS Identity and Access Management, Amazon Managed Streaming for Apache Kafka Kafka AWS Lake Formation, CloudWatch Amazon Logs AWS Elemental MediaLive, AWS Elemental MediaPackage, Amazon Relational Database Service, Amazon Simple Storage Service AWS Secrets Manager, Amazon Security Lake AWS Service Catalog, Amazon Simple Email AWS X-Ray Service y Amazon API Gateway.	28 de julio de 2025

Cambio	Descripción	Fecha
«, kafkaconnect: ListTagsF orResource «, kafkaconnect: «, kafkaconnect: ListWorke rConfigurations «, kafkaconn ect: connect: «, «kafkacon nect: DescribeLakeFormat ionIdentityCenterConfiguration «, «kafkaconnect: Describel ndexPolicies «, «lakeform ation: ListTagsForResource «, «registros: «, «medialive: DescribeMultiplexProgram«, «medialive: ListMultiplexProgr ams «, «media package v2: GetChannelGroup «, «media package v2: «, «rds: ListChannelGroups «, «roles en cualquier parte: «, GetProfil e «roles en cualquier parte: GetTrustAnchor «, «roles en cualquier parte: ListProfiles «, «roles en cualquier parte: ListTagsForResource «, «roles en cualquier lugar: ListTrust Anchors «, GetAccessGrant «s3: «, ListAccessGrants «s3: «, DescribeSecret «administrador de secretos: ListDataLakeExceptions «, «security lake: ListDataL akes «, «security lake»: ListLogSources «, «security lake: GetAttributeGroup «, «servicecatalog: «, ListAttri buteGroups «servicecatalog:		

Cambio	Descripción	Fecha
«, «servicecatalog: ListServiceActions «, «servicecatalog: ListServiceActions ForProvisioningArtifact «, «ses: DescribeEngineDefaultParameters GetTrafficPolicy «, «ses: ListTagsForResource «, «ses: ListTrafficPolicies «, «xray: GetGroup «, GetGroups «xray: «, GetSamplingRules «xray: ListResourcePolicies «, «xray: ListTagsForResource «, «xray: «, «arn:aws:apiGateway: ::/account», «arn:aws: apigateway: ::apigateway: ::/usageplans/».		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy— Añada «backup-gateway: GetHypervisor «, ListHypervisors «backup-gatewaybcm-data-exports: GetExport «,"bcm-data-exports: ListExports «,"bcm-data-exports: ListTagsForResource «, «roca madre: GetAgent «, GetAgentActionGroup «roca madre: «, GetAgentKnowledgeBase «roca madre: GetDataSource «, «roca madre: GetFlowAlias «, «roca madre: GetFlowVersion «, «roca madre: ListAgentActionGroups «, ListAgentKnowledgeBases «roca madre: «, ListDataSources «roca madre: «, ListFlowAliases «roca madre: ListFlowVersions «, «formación de nubes: BatchDescribeTypeConfigurations «, «formación de nubes: «, DescribeStackSet «formación de nubes: ListStackInstances «,» DescribeStackInstance cloudformation: ListStackSets «, «cloudfront: GetPublicKey «, «cloudfront: GetRealtimeLogConfig «, ListPublicKeys «cloudfront: «, ListRealtimeLogConfigs «cloudfro	Esta política ahora admite permisos adicionales para Amazon Bedrock AWS Backup gateway Administración de facturación y costos de AWS, Amazon,, AWS CloudFormation,, CloudFront, AWS Entity Resolution AWS IoT Core Device Advisor AWS Lambda AWS Network Manager, Amazon Relational Database Service AWS Private Certificate Authority, Amazon Redshift, Amazon S3 Tables,. Quick Setup de AWS Systems Manager	18 de junio de 2025

Cambio	Descripción	Fecha
nt: «, GetIdMappingWorkfl ow «resolución de entidad: GetSchemaMapping «, «resolución de entidad: ListIdMappingWorkflows «, «resolución de entidad: ListSchemaMappings «, «resolución de entidad: ListTagsForResource «, «iotdeviceadvisor: GetSuiteD efinition «, «iotdeviceadvisor: ListSuiteDefinitions «, GetEventSourceMapp ing «lambda: «, ListEvent SourceMappings «lambda: «, «paquete multimedia v2: GetChannel «, «paquete multimedia v2: ListChann els «, «administrador de red: GetTransitGatewayP eering «, ListPeerings «administrador de redpca-connector-ad: GetDirect oryRegistration «,» pca-conne ctor-ad: ListDirectoryRegis trations «,"pca-connector-ad: ListTagsForResource «, «rds:Describe DBShard grupos», DescribeIntegratio ns «rds: «, DescribeIntegratio ns «redshift: «, GetTableB ucket «s3tables: GetTableB ucketEncryption «, «s3tables : GetTableBucketMain tenanceConfiguration «,		

Cambio	Descripción	Fecha
«s3tables: ListTableBuckets «, «s3tables: GetConfigurationManager «, «ssm-quicksetup:ListConfigurationManagers»		

Cambio	Descripción	Fecha
AWS_ConfigRole— Añada «backup-gateway: GetHypervisor «, ListHypervisors «backup-gatewaybcm-data-exports: GetExport «,"bcm-data-exports: ListExports «,"bcm-data-exports: ListTagsForResource «, «roca madre: GetAgent «, GetAgentActionGroup «roca madre: «, GetAgentKnowledgeBase «roca madre: GetDataSource «, «roca madre: GetFlowAlias «, «roca madre: GetFlowVersion «, «roca madre: ListAgentActionGroups «, ListAgentKnowledgeBases «roca madre: «, ListDataSources «roca madre: «, ListFlowAliases «roca madre: ListFlowVersions «, «formación de nubes: BatchDescribeTypeConfigurations «, «formación de nubes: «, DescribeStackSet «formación de nubes: ListStackInstances «,» DescribeStackInstance cloudformation: ListStackSets «, «cloudfront: GetPublicKey «, «cloudfront: GetRealtimeLogConfig «, «cloudfront: ListPublicKeys «, «cloudfront: ListRealtimeLogConfigs	Esta política ahora admite permisos adicionales para Amazon Bedrock AWS Backup gateway Administración de facturación y costos de AWS, Amazon,, AWS CloudFormation,, CloudFront, AWS Entity Resolution AWS IoT Core Device Advisor AWS Lambda AWS Network Manager, Amazon Relational Database Service AWS Private Certificate Authority, Amazon Redshift, Amazon S3 Tables,. Quick Setup de AWS Systems Manager	18 de junio de 2025

Cambio	Descripción	Fecha
«, «resolución de entidad: GetIdMappingWorkflow «, GetSchemaMapping «resolución de entidad: «, ListIdMappingWorkflows «resolución de entidad: «, ListSchemaMappings «resolución de entidad: «, ListTagsForResource «iotdeviceadvisor: GetSuiteDefinition «, «iotdeviceadvisor: ListSuiteDefinitions «, «lambda: GetEventSourceMapping «, «lambda: ListEventSourceMappings «, «administrador de red: GetTransitGatewayPeering «, «administrador de redpca-connector-ad: GetDirectoryRegistration «,"pca-connector-ad: ListDirectoryRegistrations «,"pca-connector-ad: ListTagsForResource «, «rds: ListPeerings Describa DBShard los grupos», DescribeIntegrations «rds: «, DescribeIntegrations «redshift: «, GetTableBucket «s3tables: «, GetTableBucketEncryption «s3tables: GetTableBucketMaintenanceConfiguration «, «s3tables: ListTableBuckets «, «sm-quicksetup:», GetConfigurationManager		

Cambio	Descripción	Fecha
«ssm-quicksetup:ListConfigurationManagers»		
AWS_ConfigRole: añadir "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", " bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource"	Esta política ahora admite permisos adicionales para Amazon Bedrock.	27 de mayo de 2025
AWSConfigServiceRolePolicy: añadir "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", " bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource"	Esta política ahora admite permisos adicionales para Amazon Bedrock.	27 de mayo de 2025

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	Esta política ahora admite permisos adicionales para Amazon Bedrock Intercambio de datos de AWS B2B,,, AWS Database Migration Service (AWS DMS) AWS Clean Rooms AWS CodeConnections, Amazon CloudWatch Logs AWS Direct Connect, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), SageMaker Amazon AI AWS Security Hub CSPM y Contacts y. Administrador de incidentes de AWS Systems Manager Administrador de incidentes de AWS Systems Manager AWS Systems Manager	8 de abril de 2025

Cambio	Descripción	Fecha
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsFor Resource", "s3:GetAccessGra ntsInstance", "s3:GetAc cessGrantsLocation", "s3:Li stAccessGrantsInstances", "s3:ListAccessGrantsLocatio ns", "sagemaker:DescribeClu ster", "sagemaker:DescribeM lflowTrackingServer", "sage maker:DescribeStudioLifecyc leConfig", "sagemaker:ListC lusters", "sagemaker:ListMlf lowTrackingServers", "sagem aker:ListStudioLifecycleCon figs", "securityhub:Describ eStandardsControls", "secur ityhub:GetEnabledStandards" , "ssm-contacts:GetContact", "ssm-contacts:GetContactCha nnel", "ssm-contacts:ListCo ntactChannels", "ssm-cont acts:ListContacts", "ssm-in cidents:GetResponsePlan", " ssm-incidents:ListResponseP lans", "ssm-incidents:ListT agsForResource", "ssm:Descr ibeInstanceInformation"		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	Esta política ahora admite permisos adicionales para Amazon Bedrock Intercambio de datos de AWS B2B,,, AWS Database Migration Service (AWS DMS) AWS Clean Rooms AWS CodeConnections, Amazon CloudWatch Logs AWS Direct Connect, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), SageMaker Amazon AI AWS Security Hub CSPM y Contacts y. Administrador de incidentes de AWS Systems Manager Administrador de incidentes de AWS Systems Manager AWS Systems Manager Esta política ahora también admite el permiso de acceso a todos los nombres de dominio de Amazon API Gateway al incluir el patrón de recursos “`arn:aws:apigateway:::/domainnames/` ”.	8 de abril de 2025

Cambio	Descripción	Fecha
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation"		
AWS_ConfigRole: añadir "ec2:GetAllowedImagesSettings"	Esta política admite ahora permisos adicionales para Amazon Elastic Compute Cloud (Amazon EC2).	4 de marzo de 2025

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "ec2:GetAllowedImagesSettings"	Esta política admite ahora permisos adicionales para Amazon Elastic Compute Cloud (Amazon EC2).	4 de marzo de 2025
AWS_ConfigRole: añadir "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	Esta política ahora admite permisos adicionales para Amazon Comprehend AWS Clean Rooms, Amazon Elastic Compute Cloud (Amazon EC2) AWS HealthOmics, Amazon Simple Storage Service (Amazon S3) y Amazon Simple Email Service (Amazon SES).	16 de enero de 2025

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	Esta política ahora admite permisos adicionales para Amazon Comprehend AWS Clean Rooms, Amazon Elastic Compute Cloud (Amazon EC2) AWS HealthOmics, Amazon Simple Storage Service (Amazon S3) y Amazon Simple Email Service (Amazon SES).	16 de enero de 2025
AWSConfigServiceRolePolicy: añadir "organizations:ListAWSServiceAccessForOrganization"	Esta política ahora admite permisos adicionales para AWS Organizations.	18 de diciembre de 2024

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", "iot:ListThingGroups", "iot	Esta política ahora admite permisos adicionales para Amazon Connect AWS AppConfig, Amazon AWS CloudTrail, Amazon DevOps Guru, Identity Store DataZone, , AWS Glue, Amazon Interactive Video Service (Amazon IVS) AWS IoT AWS IoT FleetWise AWS IoT Wireless, Amazon Logs, Amazon Observability Access AWS Payment Cryptography Manager, CloudWatch Amazon Relational Database Service (CloudWatch Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3)) Simple Storage S3), Amazon Scheduler y Amazon VPC Lattice. EventBridge AWS Systems Manager	7 de noviembre de 2024

Cambio	Descripción	Fecha
:ListThingTypes", "iotfleet wise:GetDecoderManifest", " iotfleetwise:GetFleet", "iotfleet wise:GetModelManifest", "io tfleetwise:GetSignalCatalog ", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderMa nifestNetworkInterfaces", " iotfleetwise:ListDecoderMan ifests", "iotfleetwise:List DecoderManifestSignals", "iotfleetwise:ListFleets", "i otfleetwise:ListModelManife stNodes", "iotfleetwise:Lis tModelManifests", "iotfleet wise:ListSignalCatalogNodes ", "iotfleetwise:ListSignal Catalogs", "iotfleetwise:Li stTagsForResource", "iotfleet wise:ListVehicles", "iotwir eless:GetDestination", "iotwirel ess:GetDeviceProfile", "iot wireless:GetWirelessGateway ", "iotwireless:ListDestina tions", "iotwireless:ListDe viceProfiles", "iotwireless :ListWirelessGateways", "iv schat:GetLoggingConfigurati on", "ivschat:GetRoom" "ivschat:ListLoggingConfigu rations", "ivschat:ListRooms ", "ivschat:ListTagsForReso urce", "logs:GetLogAnomal yDetector", "logs:ListLogAn omalyDetectors", "oam:GetS		

Cambio	Descripción	Fecha
ink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType",	Esta política ahora admite permisos adicionales para Amazon Connect AWS AppConfig, Amazon AWS CloudTrail, Amazon DevOps Guru, Identity Store DataZone, , AWS Glue, Amazon Interactive Video Service (Amazon IVS) AWS IoT AWS IoT FleetWise AWS IoT Wireless, Amazon Logs, Amazon Observability Access AWS Payment Cryptography Manager, CloudWatch Amazon Relational Database Service (CloudWatch Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3)) Simple Storage S3), Amazon Scheduler y Amazon VPC Lattice. EventBridge AWS Systems Manager	7 de noviembre de 2024

Cambio	Descripción	Fecha
"iot:ListThingGroups", "iot :ListThingTypes", "iotfleet wise:GetDecoderManifest", " iotfleetwise:GetFleet", "iotfleet wise:GetModelManifest", "io tfleetwise:GetSignalCatalog ", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderMa nifestNetworkInterfaces", " iotfleetwise:ListDecoderMan ifests", "iotfleetwise:List DecoderManifestSignals", "iotfleetwise:ListFleets", "i otfleetwise:ListModelManife stNodes", "iotfleetwise:Lis tModelManifests", "iotfleet wise:ListSignalCatalogNodes ", "iotfleetwise:ListSignal Catalogs", "iotfleetwise:Li stTagsForResource", "iotfleet wise:ListVehicles", "iotwir eless:GetDestination", "iotwirel ess:GetDeviceProfile", "iot wireless:GetWirelessGateway ", "iotwireless:ListDestina tions", "iotwireless:ListDe viceProfiles", "iotwireless :ListWirelessGateways", "iv schat:GetLoggingConfigurati on", "ivschat:GetRoom" "ivschat:ListLoggingConfigu rations", "ivschat:ListRooms ", "ivschat:ListTagsForReso urce", "logs:GetLogAnomal yDetector", "logs:ListLogAn		

Cambio	Descripción	Fecha
omalyDetectors", "oam:GetSink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	Esta política ahora admite permisos adicionales para Amazon OpenSearch Service Severless, Amazon, AppStream, AWS Backup AWS CloudTrail AWS Glue, EC2 Image Builder AWS IoT, Amazon Interactive Video Service (Amazon AWS Elemental MediaConnect IVS),, AWS Elemental MediaTailor, AWS HealthOmics y Amazon Scheduler. EventBridge	16 de septiembre de 2024

Cambio	Descripción	Fecha
rictionPolicies," "ivs:List Stages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	Esta política ahora admite permisos adicionales para Amazon OpenSearch Service Severless, Amazon, AppStream, AWS Backup AWS CloudTrail AWS Glue, EC2 Image Builder AWS IoT, Amazon Interactive Video Service (Amazon AWS Elemental MediaConnect IVS),, AWS Elemental MediaTailor, AWS HealthOmics y Amazon Scheduler. EventBridge	16 de septiembre de 2024

Cambio	Descripción	Fecha
rictionPolicies," "ivs:List Stages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		
AWS_ConfigRole: añadir "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	Esta política ahora admite permisos adicionales para Amazon Elastic File System (Amazon EFS), Amazon Redshift y. AWS Systems Manager para SAP	17 de junio de 2024
AWSConfigServiceRolePolicy: añadir "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	Esta política ahora admite permisos adicionales para Amazon Elastic File System (Amazon EFS), Amazon Redshift y. AWS Systems Manager para SAP	17 de junio de 2024

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:G	Esta política ahora admite permisos adicionales para Amazon Managed Service para Prometheus, CloudWatch Amazon, Amazon Cognito, Amazon, ElastiCache Amazon, (IAM) AWS Identity and Access Management ,, FSx AWS Glue Amazon Redshift Serverless AWS Lambda AWS RAM, Amazon AI y Amazon Simple Notification Service (SageMaker Amazon SNS).	22 de febrero de 2024

Cambio	Descripción	Fecha
etSMSSandboxAccountStatus"		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and	Esta política ahora admite permisos adicionales para Amazon Managed Service para Prometheus, CloudWatch Amazon, Amazon Cognito, Amazon, ElastiCache Amazon, (IAM) AWS Identity and Access Management ,, FSx AWS Glue Amazon Redshift Serverless AWS Lambda AWS RAM, Amazon AI y Amazon Simple Notification Service (SageMaker Amazon SNS).	22 de febrero de 2024

Cambio	Descripción	Fecha
"sns:GetSMSSandboxAccountStatus"		
AWSConfigUserAccess—AWS Config comienza a realizar un seguimiento de los cambios de esta política gestionada AWS	Esta política proporciona acceso al uso AWS Config, incluida la búsqueda por etiquetas en los recursos y la lectura de todas las etiquetas . Esto no proporciona permiso de configuración AWS Config, lo que requiere privilegios administrativos.	22 de febrero de 2024
AWS_ConfigRole: añadir "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Esta política ahora admite permisos adicionales para AWS AppConfig Amazon Managed Service for Prometheus AWS Database Migration Service ,AWS DMS(), () IAM, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management(Amazon MSK) AWS Organizations, Amazon Logs y CloudWatch Amazon Simple Storage Service (Amazon S3).	5 de diciembre de 2023

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Esta política ahora admite permisos adicionales para AWS AppConfig Amazon Managed Service for Prometheus AWS Database Migration Service ,AWS DMS(), () IAM, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management(Amazon MSK) AWS Organizations, Amazon Logs y CloudWatch Amazon Simple Storage Service (Amazon S3).	5 de diciembre de 2023

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationAssociation	Esta política ahora admite permisos adicionales para Amazon Cognito, Amazon Connect, Amazon EMR, Amazon MemoryDB AWS Ground Station, AWS Mainframe Modernization Amazon Quick AWS Organizations, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53 y. AWS Service Catalog AWS Transfer Family	17 de noviembre de 2023

Cambio	Descripción	Fecha
s," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrL		

Cambio	Descripción	Fecha
ocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole: añadir "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Esta política ahora añade identificadores de seguridad (SID) para `AWSConfigServiceRolePolicyStatementID`, `AWSConfigSLRLogStatementID`, `AWSConfigSLRLogEventStatementID` y `AWSConfigSLRApiGatewayStatementID`.	17 de noviembre de 2023

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect	Esta política ahora admite permisos adicionales para Amazon Cognito, Amazon Connect, Amazon EMR, Amazon MemoryDB AWS Ground Station, AWS Mainframe Modernization Amazon Quick AWS Organizations, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53 y. AWS Service Catalog AWS Transfer Family	17 de noviembre de 2023

Cambio	Descripción	Fecha
:ListIntegrationAssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCid		

Cambio	Descripción	Fecha
rBlocks," "route53:ListCidrLocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy: añadir "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Esta política ahora añade identificadores de seguridad (SID) para `AWSConfigServiceRolePolicyStatementID`, `AWSConfigSLRLogStatementID`, `AWSConfigSLRLogEventStatementID` y `AWSConfigSLRApiGatewayStatementID`.	17 de noviembre de 2023

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListT	Esta política ahora admite permisos adicionales para Amazon Connect AWS Private CA AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon Evidentemente, CloudWatch Amazon Managed Grafana, Amazon, GuardDuty Amazon AWS IoT Inspector AWS IoT TwinMaker,, Amazon Managed Streaming for Apache Kafka (Amazon AWS Lambda MSK AWS Network Manager) AWS Organizations,,, y Amazon AI. SageMaker	4 de octubre de 2023

Cambio	Descripción	Fecha
ags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSi	Esta política ahora admite permisos adicionales para Amazon Connect AWS Private CA AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon Evidentemente, CloudWatch Amazon Managed Grafana, Amazon, GuardDuty Amazon AWS IoT Inspector AWS IoT TwinMaker,, Amazon Managed Streaming for Apache Kafka (Amazon AWS Lambda MSK AWS Network Manager) AWS Organizations,,, y Amazon AI. SageMaker	4 de octubre de 2023

Cambio	Descripción	Fecha
gningConfigs," "lambda:ListTags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy: elimina "ssm:GetParameter"	Esta política ahora elimina los permisos para AWS Systems Manager (Systems Manager).	6 de septiembre de 2023

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	Esta política ahora admite permisos adicionales para AWS App Mesh, Amazon AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact, Amazon AWS CodeBuild, AWS Identity and Access Management (IAM) AWS Glue GuardDuty, Amazon Inspector,,, Amazon Managed Streaming for Apache Kafka AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Macie,,,, Amazon Route 53 AWS Elemental MediaConnect AWS Network Manager AWS Organizations Explorador de recursos de AWS, Amazon Simple Storage Service (Amazon S3) y Amazon Simple Notification Service (Amazon SNS) Simple Service SNS).	28 de julio de 2023

Cambio	Descripción	Fecha
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	Esta política ahora admite permisos adicionales para Amazon WorkSpaces Applications AWS App Mesh, Amazon, AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact, Amazon AWS CodeBuild, AWS Identity and Access Management (IAM) AWS Glue GuardDuty, Amazon Inspector,,, Amazon Managed Streaming for Apache Kafka AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Macie,,,, , Amazon Route 53 AWS Elemental MediaConnect AWS Network Manager AWS Organizations Explorador de recursos de AWS, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Simple Notification (SNS) y Amazon EC2 Systems Manager (SSM).	28 de julio de 2023

Cambio	Descripción	Fecha
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir "amplify:GetBranch", "amplify: ListBranches", "app-integrat ions:GetEventIntegration", "app-integrations:ListEventI ntegrationAssociations", "ap p-integrations:ListEventInt egrations", "appmesh: DescribeRoute", "ap pmesh:ListRoutes", "aps:List RuleGroupsNamespaces", "athena:GetPreparedStat ement", "athena:ListPrepar edStatements", "batch:Descri beSchedulingPolicies", "batch:ListSchedulingPolici es", "cloudformation:ListTyp es", "cloudtrail:ListTrails", "co deartifact:ListDomains", "co deguru-profiler:DescribePro filingGroup", "codeguru-prof iler:GetNotificationConfigu ration", "codeguru-profiler: GetPolicy", "codeguru-profil er:ListProfilingGroups", "ds:DescribeDomainCon trollers", “dynamodb:Describ eTableReplicaAutoScaling" "dynamodb:DescribeTi meToLive", "ec2:Desc ribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	Esta política ahora admite permisos adicionales para Amazon Connect AWS Amplify, Amazon Managed Service for Prometheus AWS App Mesh, Amazon Athena,,, , Amazon, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudForm ation AWS CloudTrail AWS CodeArtifact, Amazon Elastic Compute Cloud (Amazon EC2) CodeGuru, Amazon CloudWatch Evidentemente, Amazon Forecast,,, (IAM), Amazon Managed Streaming for Apache Kafka Managed for Apache (Amazon MSK) AWS IoT Greengrass, AWS Ground Station AWS Identity and Access Management Amazon Lightsail, Amazon Logs, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC) AWS Organizations CloudWatch AWS Elemental MediaConn ect AWS Elemental MediaTail or), Amazon Personali ze, Amazon Quick AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service (Amazon S3),	13 de junio de 2023

Cambio	Descripción	Fecha
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts",	SageMaker Amazon AI,. AWS Transfer Family	

Cambio	Descripción	Fecha
"organizations:ListAccounts ForParent", "organizations:L istOrganizationalUnitsForPa rent", "organizations:ListTa gsForResource", "personal ize:DescribeDataset", "perso nalize:DescribeDatasetGroup", "personalize:DescribeSchema ", "personalize:DescribeSolu tion", "personalize:ListD atasetGroups", "personalize: ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForRe source", "quicksight:ListTe mplates", "refactor-spaces:G etEnvironment", "refactor -spaces:GetService", "refactor-spaces:ListAppl ications", "refactor-spaces: ListEnvironments", "refactor -spaces:ListServices", "s3:GetAccessPointPolic yStatusForObjectLambda", "sagemaker:DescribeDe viceFleet", "sagemake r:DescribeFeatureGroup", "sa gemaker:ListDeviceFleets", "sagemaker:ListFeatureGroup s", "sagemaker:ListModels", and "transfer:ListTags ForResource"		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast	Esta política ahora admite permisos adicionales para Amazon Connect AWS Amplify, Amazon Managed Service for Prometheus AWS App Mesh, Amazon Athena,,, , Amazon, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact, Amazon Elastic Compute Cloud (Amazon EC2) CodeGuru, Amazon CloudWatch Evidentemente, Amazon Forecast,,, (IAM), Amazon Managed Streaming for Apache Kafka Managed for Kafka (AWS Ground Station Amazon MSK) AWS IoT Greengrass, AWS Identity and Access Management Amazon Lightsail, Amazon Logs, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC) AWS Organizations CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor, Amazon Personalize, Amazon Quick AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service (Amazon S3), SageMaker	13 de junio de 2023

Cambio	Descripción	Fecha
:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:ListAccounts	Amazon AI,. AWS Transfer Family	

Cambio	Descripción	Fecha
ForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	Esta política ahora admite permisos adicionales para Amazon Managed Workflows para AWS Amplify, AWS App Mesh AWS App Runner, Amazon CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, SageMaker Amazon AWS Transfer Family AI, Amazon AWS Migration Hub Pinpoint AWS , Resilience Hub, Amazon CloudWatch, AWS Directory Service y. AWS WAF	13 de abril de 2023

Cambio	Descripción	Fecha
ion, macie2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificatio	Esta política ahora admite permisos adicionales para Amazon Managed Workflows para AWS Amplify, AWS App Mesh AWS App Runner, Amazon CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, SageMaker Amazon AWS Transfer Family AI, Amazon AWS Migration Hub Pinpoint AWS , Resilience Hub, Amazon CloudWatch, AWS Directory Service y. AWS WAF	13 de abril de 2023

Cambio	Descripción	Fecha
nExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstancePro	Esta política ahora admite permisos adicionales para Amazon Managed Workflows para Amazon AppFlow AWS App Runner, Amazon WorkSpaces Applications, Amazon CloudFront, Amazon, CloudWatch,, AWS CodeArtifact AWS CodeCommit AWS Device Farm, Amazon CloudWatch Evidentemente, Amazon Forecast, AWS Ground Station, AWS Identity and Access Management (IAM), AWS IoT Amazon MemoryDB, Amazon Pinpoint, , Amazon AWS Network Manager Relational AWS Panorama Database Service (Amazon RDS), Amazon Redshift y Amazon AI. SageMaker	30 de marzo de 2023

Cambio	Descripción	Fecha
file, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig,	Esta política ahora admite permisos adicionales para Amazon Managed Workflows for Amazon AppFlow AWS App Runner, Amazon WorkSpaces Applications, Amazon AWS CloudFormation, Amazon CloudFront, Amazon CloudWatch AWS CodeArtifact AWS CodeCommit AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidentemente, CloudWatch Amazon Forecast, (AWS IoT IAM), AWS Ground Station Amazon AWS Identity and Access Management MemoryDB, Amazon AWS Network Manager Pinpoint AWS Panorama, Amazon Evident, Amazon Relational Database Service (Amazon R DS), Amazon Redshift y Amazon AI. SageMaker	30 de marzo de 2023

Cambio	Descripción	Fecha
groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Cambio	Descripción	Fecha
AWSConfigRulesExecutionRole— comienza a realizar un seguimiento de los cambios de esta AWS Config política gestionada AWS	Esta política permite a AWS Lambda las funciones acceder a la AWS Config API y a las instantáneas de configuración que se AWS Config envían periódicamente a Amazon S3. Las funciones que evalúan los cambios de configuración de las reglas Lambda AWS personalizadas requieren este acceso.	7 de marzo de 2023
AWSConfigRoleForOrganizations— AWS Config comienza a realizar un seguimiento de los cambios de esta política AWS gestionada	Esta política permite AWS Config realizar llamadas de solo lectura AWS Organizations APIs.	7 de marzo de 2023
AWSConfigRemediationServiceRolePolicy— AWS Config comienza a rastrear los cambios de esta política gestionada AWS	Esta política permite AWS Config corregir `NON_COMPLIANT` los recursos en su nombre.	7 de marzo de 2023
AWSConfigServiceRolePolicy: añadir auditmanager:GetAccountStatus	Esta política ahora permite devolver el estado de registro de una cuenta en AWS Audit Manager.	3 de marzo de 2023
AWS_ConfigRole: añadir auditmanager:GetAccountStatus	Esta política ahora permite devolver el estado de registro de una cuenta en AWS Audit Manager.	3 de marzo de 2023

Cambio	Descripción	Fecha
AWSConfigMultiAccountSetupPolicy— AWS Config comienza a realizar un seguimiento de los cambios de esta política AWS gestionada	Esta política permite llamar AWS Config a AWS los servicios e implementar AWS Config recursos en una organización con AWS Organizations.	27 de febrero de 2023

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Esta política ahora admite permisos adicionales para Amazon Managed Workflows para Apache Airflow, AWS IoT Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer, Amazon Kinesis Video Streams AWS HealthLake, Amazon Application Recovery Controller (ARC), Amazon Elastic Compute Cloud (AWS Device Farm Amazon EC2) Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM), Amazon y Amazon Logs. GuardDuty CloudWatch	1 de febrero de 2023

Cambio	Descripción	Fecha
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Esta política ahora admite permisos adicionales para Amazon Managed Workflows para Apache Airflow, AWS IoT Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer, Amazon Kinesis Video Streams AWS HealthLake, Amazon Application Recovery Controller (ARC), Amazon Elastic Compute Cloud (AWS Device Farm Amazon EC2) Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM), Amazon y Amazon Logs. GuardDuty CloudWatch	1 de febrero de 2023

Cambio	Descripción	Fecha
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy: actualizar config:DescribeConfigRules	Como práctica recomendada de seguridad, ahora esta política elimina el permiso amplio en el nivel de los recursos para `config:DescribeConfigRules` .	12 de enero de 2023

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	Esta política ahora admite permisos adicionales para Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2 AWS Glue) AWS Directory Service,, Amazon Lightsail AWS IoT,, Amazon Quick, AWS Elemental MediaPackage Amazon AWS Network Manager Application Recovery Controller (ARC), AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) y Amazon Timestream Timestream.	15 de diciembre de 2022

Cambio	Descripción	Fecha
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	Esta política ahora admite permisos adicionales para Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2 AWS Glue) AWS Directory Service,, Amazon Lightsail AWS IoT,, Amazon Quick, AWS Elemental MediaPackage Amazon AWS Network Manager Application Recovery Controller (ARC), AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) y Amazon Timestream Timestream.	15 de diciembre de 2022

Cambio	Descripción	Fecha
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir cloudformation:ListStackResources and cloudformation:ListStacks	Esta política ahora otorga permiso para devolver descripciones de todos los recursos de una AWS CloudFormation pila específica y devolver la información resumida de las pilas cuyo estado coincida con el especificadoStackStatusFilter.	7 de noviembre de 2022
AWS_ConfigRole: añadir cloudformation:ListStackResources and cloudformation:ListStacks	Esta política ahora permite devolver las descripciones de todos los recursos de una AWS CloudFormation pila específica y devolver la información resumida de las pilas cuyo estado coincida con el especificado. StackStatusFilter	7 de noviembre de 2022

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Esta política ahora admite permisos adicionales para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow, Amazon Keyspaces, AWS AppConfig Amazon AWS Amplify, Amazon Connect, Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, EventBridge Amazon AWS Fault Injection Service, Amazon Servers, Amazon Location AWS IoT Service, FSx Amazon Lex GameLift , Amazon Lightsail, Amazon Pinpoint, Amazon Quick, Amazon Relational Database Service (Amazon OpsWorks) CloudWatch AWS Panorama AWS Resource Access Manager RDS), Amazon AWS RoboMaker Rekognition, Amazon Route 53 Grupos de recursos de AWS, Amazon Simple Storage Service (Amazon S3) y. AWS Cloud Map AWS Security Token Service	19 de octubre de 2022

Cambio	Descripción	Fecha
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Cambio	Descripción	Fecha
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Cambio	Descripción	Fecha
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Esta política ahora admite permisos adicionales para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow, Amazon Keyspaces, AWS AppConfig Amazon AWS Amplify, Amazon Connect, Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, EventBridge Amazon AWS Fault Injection Service, Amazon Servers, Amazon Location AWS IoT Service, FSx Amazon Lex GameLift , Amazon Lightsail, Amazon Pinpoint, Amazon Quick, Amazon Relational Database Service (Amazon OpsWorks) CloudWatch AWS Panorama AWS Resource Access Manager RDS), Amazon AWS RoboMaker Rekognition, Amazon Route 53 Grupos de recursos de AWS, Amazon Simple Storage Service (Amazon S3) y. AWS Cloud Map AWS Security Token Service	19 de octubre de 2022

Cambio	Descripción	Fecha
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Cambio	Descripción	Fecha
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Cambio	Descripción	Fecha
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir Glue::GetTable	Esta política ahora otorga permiso para recuperar la definición de AWS Glue tabla en un catálogo de datos para una tabla específica.	14 de septiembre de 2022
AWS_ConfigRole: añadir Glue::GetTable	Esta política ahora otorga permiso para recuperar la definición de AWS Glue tabla en un catálogo de datos para una tabla específica.	14 de septiembre de 2022

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	Esta política ahora admite permisos adicionales para Amazon AppFlow, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas, Amazon Fraud Detector, EventBridge Amazon Servers, Amazon FinSpace Amazon Interactive Video Service (Amazon IVS) GameLift , Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service , Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon Quick, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), Amazon Simple	7 de septiembre de 2022

Cambio	Descripción	Fecha
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Amazon Route 53 Resolver Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation, AWS License Manager AWS Resilience Hub, AWS Signer, y AWS Transfer Family.	

Cambio	Descripción	Fecha
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

Cambio	Descripción	Fecha
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

Cambio	Descripción	Fecha
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

Cambio	Descripción	Fecha
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

Cambio	Descripción	Fecha
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

Cambio	Descripción	Fecha
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

Cambio	Descripción	Fecha
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

Cambio	Descripción	Fecha
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	Esta política ahora admite permisos adicionales para Amazon AppFlow, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas, Amazon Fraud Detector, EventBridge Amazon Servers, Amazon FinSpace Amazon Interactive Video Service (Amazon IVS) GameLift , Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service , Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon Quick, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), Amazon Simple	7 de septiembre de 2022

Cambio	Descripción	Fecha
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	Amazon Route 53 Resolver Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation AWS License Manager AWS Resilience Hub AWS Signer AWS Transfer Family	

Cambio	Descripción	Fecha
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

Cambio	Descripción	Fecha
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

Cambio	Descripción	Fecha
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

Cambio	Descripción	Fecha
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

Cambio	Descripción	Fecha
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

Cambio	Descripción	Fecha
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

Cambio	Descripción	Fecha
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

Cambio	Descripción	Fecha
ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject,	Esta política ahora admite permisos adicionales para Amazon Managed Workflows para Apache Airflow, AWS IoT Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer, Amazon Kinesis Video Streams AWS HealthLake, Amazon Application Recovery Controller (ARC), Amazon Elastic Compute Cloud (AWS Device Farm Amazon EC2) Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM), Amazon y Amazon Logs. GuardDuty CloudWatch	1 de febrero de 2023

Cambio	Descripción	Fecha
devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Esta política ahora admite permisos adicionales para Amazon Managed Workflows para Apache Airflow, AWS IoT Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer, Amazon Kinesis Video Streams AWS HealthLake, Amazon Application Recovery Controller (ARC), Amazon Elastic Compute Cloud (AWS Device Farm Amazon EC2) Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM), Amazon y Amazon Logs. GuardDuty CloudWatch	1 de febrero de 2023

Cambio	Descripción	Fecha
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy: actualizar config:DescribeConfigRules	Como práctica recomendada de seguridad, ahora esta política elimina el permiso amplio en el nivel de los recursos para `config:DescribeConfigRules` .	12 de enero de 2023

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	Esta política ahora admite permisos adicionales para Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2 AWS Glue) AWS Directory Service,, Amazon Lightsail AWS IoT,, Amazon Quick, AWS Elemental MediaPackage Amazon AWS Network Manager Application Recovery Controller (ARC), AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) y Amazon Timestream Timestream.	15 de diciembre de 2022

Cambio	Descripción	Fecha
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	Esta política ahora admite permisos adicionales para Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2 AWS Glue) AWS Directory Service,, Amazon Lightsail AWS IoT,, Amazon Quick, AWS Elemental MediaPackage Amazon AWS Network Manager Application Recovery Controller (ARC), AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) y Amazon Timestream Timestream.	15 de diciembre de 2022

Cambio	Descripción	Fecha
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir cloudformation:ListStackResources and cloudformation:ListStacks	Esta política ahora otorga permiso para devolver descripciones de todos los recursos de una AWS CloudFormation pila específica y devolver la información resumida de las pilas cuyo estado coincida con el especificadoStackStatusFilter.	7 de noviembre de 2022
AWS_ConfigRole: añadir cloudformation:ListStackResources and cloudformation:ListStacks	Esta política ahora permite devolver las descripciones de todos los recursos de una AWS CloudFormation pila específica y devolver la información resumida de las pilas cuyo estado coincida con el especificado. StackStatusFilter	7 de noviembre de 2022

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Esta política ahora admite permisos adicionales para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow, Amazon Keyspaces, AWS AppConfig Amazon AWS Amplify, Amazon Connect, Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, EventBridge Amazon AWS Fault Injection Service, Amazon Servers, Amazon Location AWS IoT Service, FSx Amazon Lex GameLift , Amazon Lightsail, Amazon Pinpoint, Amazon Quick, Amazon Relational Database Service (Amazon OpsWorks) CloudWatch AWS Panorama AWS Resource Access Manager RDS), Amazon AWS RoboMaker Rekognition, Amazon Route 53 Grupos de recursos de AWS, Amazon Simple Storage Service (Amazon S3) y. AWS Cloud Map AWS Security Token Service	19 de octubre de 2022

Cambio	Descripción	Fecha
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Cambio	Descripción	Fecha
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Cambio	Descripción	Fecha
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Esta política ahora admite permisos adicionales para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow, Amazon Keyspaces, AWS AppConfig Amazon AWS Amplify, Amazon Connect, Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, EventBridge Amazon AWS Fault Injection Service, Amazon Servers, Amazon Location AWS IoT Service, FSx Amazon Lex GameLift , Amazon Lightsail, Amazon Pinpoint, Amazon Quick, Amazon Relational Database Service (Amazon OpsWorks) CloudWatch AWS Panorama AWS Resource Access Manager RDS), Amazon AWS RoboMaker Rekognition, Amazon Route 53 Grupos de recursos de AWS, Amazon Simple Storage Service (Amazon S3) y. AWS Cloud Map AWS Security Token Service	19 de octubre de 2022

Cambio	Descripción	Fecha
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Cambio	Descripción	Fecha
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Cambio	Descripción	Fecha
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir Glue::GetTable	Esta política ahora otorga permiso para recuperar la definición de AWS Glue tabla en un catálogo de datos para una tabla específica.	14 de septiembre de 2022
AWS_ConfigRole: añadir Glue::GetTable	Esta política ahora otorga permiso para recuperar la definición de AWS Glue tabla en un catálogo de datos para una tabla específica.	14 de septiembre de 2022

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	Esta política ahora admite permisos adicionales para Amazon AppFlow, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas, Amazon Fraud Detector, EventBridge Amazon Servers, Amazon FinSpace Amazon Interactive Video Service (Amazon IVS) GameLift , Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service , Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon Quick, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), Amazon Simple	7 de septiembre de 2022

Cambio	Descripción	Fecha
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Amazon Route 53 Resolver Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation, AWS License Manager AWS Resilience Hub, AWS Signer, y AWS Transfer Family.	

Cambio	Descripción	Fecha
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

Cambio	Descripción	Fecha
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

Cambio	Descripción	Fecha
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

Cambio	Descripción	Fecha
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

Cambio	Descripción	Fecha
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

Cambio	Descripción	Fecha
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

Cambio	Descripción	Fecha
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

Cambio	Descripción	Fecha
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	Esta política ahora admite permisos adicionales para Amazon AppFlow, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas, Amazon Fraud Detector, EventBridge Amazon Servers, Amazon FinSpace Amazon Interactive Video Service (Amazon IVS) GameLift , Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service , Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon Quick, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), Amazon Simple	7 de septiembre de 2022

Cambio	Descripción	Fecha
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	Amazon Route 53 Resolver Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation AWS License Manager AWS Resilience Hub AWS Signer AWS Transfer Family	

Cambio	Descripción	Fecha
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

Cambio	Descripción	Fecha
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

Cambio	Descripción	Fecha
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

Cambio	Descripción	Fecha
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

Cambio	Descripción	Fecha
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

Cambio	Descripción	Fecha
olicies, route53-recovery-r eadiness:GetCell, route53-r ecovery-readiness:GetReadin essCheck, route53-recovery- readiness:GetRecoveryGroup, route53-recovery-readiness :GetResourceSet, route53- recovery-readiness:ListCells, route53-recovery-readiness :ListReadinessChecks, route53-recovery-readin ess:ListRecoveryGroups, rou te53-recovery-readiness:Lis tResourceSets, route53resol ver:GetFirewallDomainList, route53resolver:GetFirewall RuleGroup, route53resolver: GetFirewallRuleGroupAssocia tion, route53resolver:GetRe solverQueryLogConfig, route53resolver:ListFir ewallDomainLists, route53re solver:ListFirewallDomains, route53resolver:ListFirewa llRuleGroupAssociations, ro ute53resolver:ListFirewallR uleGroups, route53resolver: ListFirewallRules, route53r esolver:ListResolverQueryLo gConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:Li stTagsForResource, s3- outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

Cambio	Descripción	Fecha
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

Cambio	Descripción	Fecha
ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		
AWSConfigServiceRolePolicy: añadir datasync:ListAgents, datasync:ListLocations, dat async:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	Esta política ahora otorga permiso para devolver una lista de AWS DataSync agentes, ubicaciones de DataSync origen y destino y DataSync tareas en una Cuenta de AWS; enumerar información resumida sobre los AWS Cloud Map espac ios de nombres y servicios que están asociados a uno o más espacios de nombres específicos en una Cuenta de AWS; y enumerar todas las listas de contactos de Amazon Simple Email Service (Amazon SES) disponibles en. Cuenta de AWS	22 de agosto de 2022

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir datasync:ListAgents, datasync:ListLocations, dat async:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	Esta política ahora otorga permiso para devolver una lista de AWS DataSync agentes, ubicaciones de DataSync origen y destino y DataSync tareas en una Cuenta de AWS; enumerar información resumida sobre los AWS Cloud Map espac ios de nombres y servicios que están asociados a uno o más espacios de nombres específicos en una Cuenta de AWS; y enumerar todas las listas de contactos de Amazon Simple Email Service (Amazon SES) disponibles en. Cuenta de AWS	22 de agosto de 2022
ConfigConformsServ iceRolePolicy: añadir cloudwatch:PutMetricData	Esta política ahora otorga permiso para publicar puntos de datos métricos en Amazon CloudWatch.	25 de julio de 2022

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	Esta política ahora admite permisos adicionales para Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon, Amazon ElastiCache EventBridge, Amazon Managed Service for Apache Flink FSx, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon Quick, Amazon Rekognition, Amazon Simple Storage Service (AWS RoboMaker Amazon S3) S3), Amazon Simple Email Service (Amazon SES),,,,,,, (IAM Identity Center AWS Amplify AWS Firewall Manager) AWS AppConfig AWS Glue AWS IAM Identity Center , EC2 Image Builder y Elastic Load Balancing. AWS AppSync AWS Billing Conductor AWS DataSync	15 de julio de 2022

Cambio	Descripción	Fecha
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

Cambio	Descripción	Fecha
ions, imagebuilder: ListCompo nents, imagebuilder:GetDist ributionConfiguration, imag ebuilder:GetInfrastructureC onfiguration, imagebuilder: ListDistributionConfigurati ons, imagebuilder:ListInfra structureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kines isanalytics:DescribeApplica tion, kinesisanalytics:List TagsForResource, quicksight :DescribeDataSource, quicksight:DescribeDataS ourcePermissions, quicksigh t:ListTagsForResource, reko gnition:DescribeStreamProce ssor, rekognition:ListTagsF orResource, robomaker:Descr ibeRobotApplication, roboma ker:DescribeSimulationAppli cation, s3:GetStorageLensCo nfiguration, s3:GetStorageL ensConfigurationTagging, se rvicediscovery:GetInstance, servicediscovery:GetNamespa ce, servicediscovery:GetSer vice, servicediscovery:List TagsForResource, ses:Descr ibeReceiptRule, ses:Describ eReceiptRuleSet, ses:GetCo ntactList, ses:GetEmailTemp late, ses:GetTemplate, and		

Cambio	Descripción	Fecha
sso:GetInlinePolicyForPermissionSet		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	Esta política ahora admite permisos adicionales para Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon, Amazon ElastiCache EventBridge, Amazon Managed Service for Apache Flink FSx, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon Quick, Amazon Rekognition, Amazon Simple Storage Service (AWS RoboMaker Amazon S3) S3), Amazon Simple Email Service (Amazon SES),,,,,,, (IAM Identity Center AWS Amplify AWS Firewall Manager) AWS AppConfig AWS Glue AWS IAM Identity Center , EC2 Image Builder y Elastic Load Balancing. AWS AppSync AWS Billing Conductor AWS DataSync	15 de julio de 2022

Cambio	Descripción	Fecha
scribeLocationS3, datasync: DescribeLocationSmb, datasy nc:DescribeTask, datasync: ListTagsForResource, ecr:De scribePullThroughCacheRules , ecr:DescribeRegistry, ecr:G etRegistryPolicy, elasticac he:DescribeCacheParameters, elasticloadbalancing:Descr ibeListenerCertificates, el asticloadbalancing:Describe TargetGroupAttributes, elas ticloadbalancing:DescribeTa rgetGroups, elasticloadbala ncing:DescribeTargetHealth, events:DescribeApiDestinat ion, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListP olicies, fms:ListTagsForRes ource, fsx:DescribeVolumes, geo:DescribeGeofenceColl ection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator , geo:DescribeTracker, geo:ListTrackerConsumers, g lue:BatchGetJobs, glue:Batc hGetWorkflows, glue:GetC rawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuil der: GetComponent, imagebuil der: ListComponentBuildVers ions, imagebuilder: ListCompo		

Cambio	Descripción	Fecha
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

Cambio	Descripción	Fecha
sso:GetInlinePolicyForPermissionSet		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	Esta política ahora otorga permiso para obtener un catálogo de datos de Amazon Athena específico, enumerar los catálogos de datos de Athena en un recurso y enumerar las etiquetas asociadas a un Cuenta de AWS grupo de trabajo o catálogo de datos de Athena; para obtener una lista de gráficos de comportamiento de Amazon Detective y etiquetas de lista para un gráfico de comportamiento de Detective; obtener una lista de metadatos de recursos para una lista determina da de nombres de puntos de enlace de desarrollo, obtener información sobre un punto final de AWS Glue desarrollo específico, obtener todo el AWS Glue AWS Glue desarrollo puntos finales en un, recuperan una seguridad específica Cuenta de AWS AWS Glue configuración, obtener todas las configuraciones de AWS Glue seguridad, obtener una lista de etiquetas asociadas a un AWS Glue recurso, obtener información sobre un	31 de mayo de 2022

Cambio	Descripción	Fecha
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	AWS Glue grupo de trabajo con el nombre especificado, recuperar los nombres de todos los recursos del AWS Glue rastreador de una AWS cuenta, obtener los nombres de todos los AWS Glue `DevEndpoint` recursos de una Cuenta de AWS, enumerar los nombres de todos los recursos de AWS Glue trabajo en una Cuenta de AWS, obtener detalles sobre las cuentas de los AWS Glue miembros, enumerar los nombres de los AWS Glue flujos de trabajo creados en una cuenta y enumerar AWS Glue los grupos de trabajo disponibles para una cuenta; recuperar detalles sobre un GuardDuty filtro de Amazon, recuperar un GuardDuty IPSet, recuperar cuentas de GuardDuty miembros, obtener una lista de GuardDuty filtros, obtener el GuardDuty servicio, recuperar las etiquetas IPSets del Servicio y obtener el ThreatIntelSets del GuardDuty GuardDuty servicio; obtener el estado actual y los ajustes de configuración de una cuenta de Amazon Macie; recuperar el recurso y las	

Cambio	Descripción	Fecha
	asociaciones principal es para AWS Resource Access Manager (AWS RAM) recursos compartidos y recuperar detalles sobre el recurso GuardDuty ThreatIntelSet AWS RAM shares; para obtener información sobre un conjunto de configuraciones existente de Amazon Simple Email Service (Amazon SES), obtener una lista de los destinos de eventos que están asociados a un conjunto de configuraciones de Amazon SES y una lista de todos los conjuntos de configuraciones asociados a una cuenta de Amazon SES; y para obtener una lista de los atributos del directorio de Identity Center, obtener los detalles de AWS IAM Identity Center un conjunto de permisos, obtener la política gestionada de IAM que se adjunta a una identidad de IAM específica Centrar el conjunto de permisos, obtener los permisos establecidos para una instancia del IAM Identity Center y obtener etiquetas para la identidad de IAM Recursos del centro.	

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	Esta política ahora otorga permiso para obtener un catálogo de datos de Amazon Athena específico, enumerar los catálogos de datos de Athena en un recurso y enumerar las etiquetas asociadas a un Cuenta de AWS grupo de trabajo o catálogo de datos de Athena; para obtener una lista de gráficos de comportamiento de Amazon Detective y etiquetas de lista para un gráfico de comportamiento de Detective; obtener una lista de metadatos de recursos para una lista determina da de nombres de puntos de enlace de desarrollo, obtener información sobre un punto final de AWS Glue desarrollo específico, obtener todo el AWS Glue AWS Glue desarrollo puntos finales en un, recuperan una seguridad específica Cuenta de AWS AWS Glue configuración, obtener todas las configuraciones de AWS Glue seguridad, obtener una lista de etiquetas asociadas a un AWS Glue recurso, obtener información sobre un	31 de mayo de 2022

Cambio	Descripción	Fecha
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	AWS Glue grupo de trabajo con el nombre especificado, recuperar los nombres de todos los recursos del AWS Glue rastreador de una AWS cuenta, obtener los nombres de todos los AWS Glue `DevEndpoint` recursos de una Cuenta de AWS, enumerar los nombres de todos los recursos de AWS Glue trabajo en una Cuenta de AWS, obtener detalles sobre las cuentas de los AWS Glue miembros, enumerar los nombres de los AWS Glue flujos de trabajo creados en una cuenta y enumerar AWS Glue los grupos de trabajo disponibles para una cuenta; recuperar detalles sobre un GuardDuty filtro de Amazon, recuperar un GuardDuty IPSet, recuperar cuentas de GuardDuty miembros, obtener una lista de GuardDuty filtros, obtener el GuardDuty servicio, recuperar las etiquetas IPSets del Servicio y obtener el ThreatIntelSets del GuardDuty GuardDuty servicio; obtener el estado actual y los ajustes de configuración de una cuenta de Amazon Macie; recuperar el recurso y las	

Cambio	Descripción	Fecha
	asociaciones principal es para AWS Resource Access Manager (AWS RAM) recursos compartidos y recuperar detalles sobre el recurso GuardDuty ThreatIntelSet AWS RAM shares; para obtener información sobre un conjunto de configuraciones existente de Amazon Simple Email Service (Amazon SES), obtener una lista de los destinos de eventos que están asociados a un conjunto de configuraciones de Amazon SES y una lista de todos los conjuntos de configuraciones asociados a una cuenta de Amazon SES; y para obtener una lista de los atributos del directorio de Identity Center, obtener los detalles de AWS IAM Identity Center un conjunto de permisos, obtener la política gestionada de IAM que se adjunta a una identidad de IAM específica Centrar el conjunto de permisos, obtener los permisos establecidos para una instancia del IAM Identity Center y obtener etiquetas para la identidad de IAM Recursos del centro.	

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Esta política ahora otorga permiso para obtener información sobre todos los almacenes de datos de AWS CloudTrail eventos (EDS) o sobre uno específico, obtener información sobre todos o un AWS CloudFormation recurso específico, obtener una lista de un grupo de parámetros o un grupo de subredes de DynamoDB Accelerator (DAX), obtener información AWS Database Migration Service sobre AWS DMS() las tareas de replicación de su cuenta en la región actual a la que se está accediendo y obtener una lista de todas las políticas de un tipo específico. AWS Organizations	7 de abril de 2022

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Esta política ahora otorga permiso para obtener información sobre todos los almacenes de datos de AWS CloudTrail eventos (EDS) o sobre uno específico, obtener información sobre todos o un AWS CloudFormation recurso específico, obtener una lista de un grupo de parámetros o un grupo de subredes de DynamoDB Accelerator (DAX), obtener información AWS Database Migration Service sobre AWS DMS() las tareas de replicación de su cuenta en la región actual a la que se está accediendo y obtener una lista de todas las políticas de un tipo específico. AWS Organizations	7 de abril de 2022

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	Esta política ahora admite permisos adicionales para DynamoDB Accelerator AWS Backup AWS Batch, Amazon DynamoDB, AWS Database Migration Service Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon, Amazon, Amazon, Amazon, Amazon, Amazon Relational Database Service, V2 y FSx GuardDuty Amazon AWS Key Management Service. AWS OpsWorks AWS WAF WorkSpaces	14 de marzo de 2022

Cambio	Descripción	Fecha
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	Esta política ahora admite permisos adicionales para DynamoDB Accelerator AWS Backup AWS Batch, Amazon DynamoDB, AWS Database Migration Service Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon, Amazon, Amazon, Amazon, Amazon, Amazon Relational Database Service, V2 y FSx GuardDuty Amazon AWS Key Management Service. AWS OpsWorks AWS WAF WorkSpaces	14 de marzo de 2022

Cambio	Descripción	Fecha
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy: añadir elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Esta política ahora otorga permiso para obtener detalles sobre los entornos de Elastic Beanstalk y una descripción de la configuración del conjunto de configuraciones de Elastic Beanstalk especificado, obtener un mapa o las versiones de Elasticsearch, describir los grupos de opciones OpenSearch de Amazon RDS disponibles para una base de datos y obtener información sobre una configuración de implementación. CodeDeploy Esta política ahora también otorga permiso para recuperar el contacto alternativo especificado adjunto a una Cuenta de AWS, recuperar información sobre una AWS Organizations política, recuperar una política de repositorio de Amazon ECR, recuperar información sobre una AWS Config regla archivada, recuperar una lista de familias de definiciones de tareas de Amazon ECS, enumerar las unidades organizativas raíz o principal (OUs) de la OU o cuenta secundaria especificada y enumerar las políticas que	10 de febrero de 2022

Cambio	Descripción	Fecha
	se adjuntan a la raíz, unidad organizativa o cuenta de destino especificada.	

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Esta política ahora otorga permiso para obtener detalles sobre los entornos de Elastic Beanstalk y una descripción de la configuración del conjunto de configuraciones de Elastic Beanstalk especificado, obtener un mapa o las versiones de Elasticsearch, describir los grupos de opciones OpenSearch de Amazon RDS disponibles para una base de datos y obtener información sobre una configuración de implementación. CodeDeploy Esta política ahora también otorga permiso para recuperar el contacto alternativo especificado adjunto a una Cuenta de AWS, recuperar información sobre una AWS Organizations política, recuperar una política de repositorio de Amazon ECR, recuperar información sobre una AWS Config regla archivada, recuperar una lista de familias de definiciones de tareas de Amazon ECS, enumerar las unidades organizativas raíz o principal (OUs) de la OU o cuenta secundaria especificada y enumerar las políticas que	10 de febrero de 2022

Cambio	Descripción	Fecha
	se adjuntan a la raíz, unidad organizativa o cuenta de destino especificada.	
AWSConfigServiceRolePolicy: añadir logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Esta política ahora otorga permiso para crear grupos de CloudWatch registros y transmisiones de Amazon y para escribir registros en transmisiones de registros creadas.	15 de diciembre de 2021
AWS_ConfigRole: añadir logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Esta política ahora otorga permiso para crear grupos de CloudWatch registros y transmisiones de Amazon y para escribir registros en transmisiones de registros creadas.	15 de diciembre de 2021
AWSConfigServiceRolePolicy: añadir es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Esta política ahora otorga permiso para obtener detalles sobre un Amazon OpenSearch Service (OpenSearch Servicio) domain/domains y obtener una lista de parámetros detallada para un grupo de parámetros de base de datos de Amazon Relational Database Service (Amazon RDS) concreto. Esta política también otorga permiso para obtener detalles sobre las instantáneas de Amazon ElastiCache .	8 de septiembre de 2021

Cambio	Descripción	Fecha
AWS_ConfigRole: añadir es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Esta política ahora otorga permiso para obtener detalles sobre un Amazon OpenSearch Service (OpenSearch Servicio) domain/domains y obtener una lista de parámetros detallada para un grupo de parámetros de base de datos de Amazon Relational Database Service (Amazon RDS) concreto. Esta política también otorga permiso para obtener detalles sobre las instantáneas de Amazon ElastiCache .	8 de septiembre de 2021

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy— Añadir logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine permisos y permisos adicionales para los tipos de recursos AWS	Esta política ahora otorga permiso para enumerar las etiquetas de un grupo de registro, enumerar las etiquetas de una máquina de estado y enumerar todas las máquinas de estado. Esta política ahora otorga permiso para obtener información sobre una máquina de estado. Esta política ahora también admite permisos adicionales para Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon, Amazon Data Firehose FSx, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon AI, Amazon Simple Notification Service, SageMaker y. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	28 de julio de 2021

Cambio	Descripción	Fecha
AWS_ConfigRole— Agregue l ogs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine y permisos adicionales para los tipos de recursos AWS	Esta política ahora otorga permiso para enumerar las etiquetas de un grupo de registro, enumerar las etiquetas de una máquina de estado y enumerar todas las máquinas de estado. Esta política ahora otorga permiso para obtener informaci ón sobre una máquina de estado. Esta política ahora también admite permisos adicionales para Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon, Amazon Data Firehose FSx, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon AI, Amazon Simple Notificat ion Service, SageMaker y. AWS Database Migration Service AWS Global Accelerat or AWS Storage Gateway	28 de julio de 2021

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy— Añadir permisos y permisos adicionales para los tipos de recursos ssm:DescribeDocumentPermission AWS	Esta política ahora otorga permiso para ver los permisos de los documentos y la información de AWS Systems Manager sobre el Analizador de acceso de IAM. Esta política ahora admite tipos de AWS recursos adicionales para Amazon Kinesis, Amazon, ElastiCache Amazon EMR, Amazon Route 53 y AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Estos cambios de permisos permiten AWS Config invocar el código de solo lectura necesario para admitir estos tipos de recursosAPIs . Esta política ahora también admite el filtrado de funciones de Lambda @Edge para la regla lambda-inside-vpc AWS Config administrada.	8 de junio de 2021

Cambio	Descripción	Fecha
AWS_ConfigRole— Añadir ssm:DescribeDocumentPermission permisos adicionales para los tipos de AWS recursos	Esta política ahora otorga permiso para ver los permisos de los documentos y la información de AWS Systems Manager sobre el Analizador de acceso de IAM. Esta política ahora admite tipos de AWS recursos adicionales para Amazon Kinesis, Amazon, ElastiCache Amazon EMR, Amazon Route 53 y AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Estos cambios de permisos permiten AWS Config invocar el código de solo lectura necesario para admitir estos tipos de recursosAPIs . Esta política ahora también admite el filtrado de funciones de Lambda @Edge para la regla lambda-inside-vpc AWS Config administrada.	8 de junio de 2021

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy— Añadir apigateway:GET permiso para realizar llamadas GET de solo lectura a API Gateway y s3:GetAccessPointPolicy permiso y s3:GetAccessPointPolicyStatus permiso para invocar Amazon S3 de solo lectura APIs	Esta política ahora otorga permisos que permiten AWS Config realizar llamadas GET de solo lectura a API Gateway para admitir una AWS Config regla para API Gateway. La política también añade permisos que permiten AWS Config invocar Amazon Simple Storage Service (Amazon S3) en modo de APIs solo lectura, que son necesarios para admitir el nuevo tipo de recurso. `AWS::S3::AccessPoint`	10 de mayo de 2021
AWS_ConFigrole: añade apigateway:GET permiso para realizar llamadas GET de solo lectura a API Gateway y s3:GetAccessPointPolicy permiso y permiso para s3:GetAccessPointPolicyStatus invocar Amazon S3 de solo lectura APIs	Esta política ahora otorga permisos que permiten AWS Config realizar llamadas GET de solo lectura a API Gateway para admitir una AWS Config API Gateway. La política también añade permisos que permiten AWS Config invocar Amazon Simple Storage Service (Amazon S3) en modo de APIs solo lectura, que son necesarios para admitir el nuevo tipo de recurso. `AWS::S3::AccessPoint`	10 de mayo de 2021

Cambio	Descripción	Fecha
AWSConfigServiceRolePolicy— Añadir ssm:ListDocuments permisos y permisos adicionales para los tipos de recursos AWS	Esta política ahora otorga permisos para ver información sobre los documentos específicos de AWS Systems Manager . Esta política ahora también admite tipos de AWS recursos adicionales para AWS Backup Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis, Amazon AI y Amazon Route SageMaker 53. AWS Database Migration Service Estos cambios de permisos permiten AWS Config invocar el código de solo lectura APIs necesario para admitir estos tipos de recursos.	1 de abril de 2021

Cambio	Descripción	Fecha
AWS_ConfigRole— Añadir ssm:ListDocuments permisos y permisos adicionales para los tipos de recursos AWS	Esta política ahora otorga permisos para ver informaci ón sobre los documentos específicos de AWS Systems Manager . Esta política ahora también admite tipos de AWS recursos adicionales para AWS Backup Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis, Amazon AI y Amazon Route SageMaker 53. AWS Database Migration Service Estos cambios de permisos permiten AWS Config invocar el código de solo lectura APIs necesario para admitir estos tipos de recursos.	1 de abril de 2021
`AWSConfigRole` está obsoleto.	`AWSConfigRole` está obsoleto. La política de reemplazo es `AWS_Confi gRole` .	1 de abril de 2021
AWS Config comenzó a rastrear los cambios	AWS Config comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	1 de abril de 2021

Permisos para el rol de IAM asignado a AWS Config

Un rol de IAM le permite definir un conjunto de permisos. AWS Config asume la función que se le asigna para escribir en su bucket de S3, publicar en su tema de SNS y realizar solicitudes `Describe` o solicitudes a la `List` API para obtener detalles de configuración de sus AWS recursos. Para obtener más información acerca de los roles de IAM, consulte Roles de IAM en la guía del usuario de IAM.

Cuando utilizas la AWS Config consola para crear o actualizar un rol de IAM, te asigna AWS Config automáticamente los permisos necesarios. Para obtener más información, consulte Configuración de AWS Config con la consola.

> **Políticas y resultados de cumplimiento**
>
> Las políticas de IAM y otras políticas administradas en AWS Organizations pueden afectar a los permisos de AWS Config para registrar cambios de configuración para los recursos. Además, las reglas evalúan directamente la configuración de un recurso y no tienen en cuenta estas políticas al ejecutar las evaluaciones. Asegúrese de que las políticas en vigor se ajusten a la forma en que piensa utilizar AWS Config.

Contenido

- Creación de políticas de roles de IAM
  - Adición de una política de confianza de IAM a su rol
  - Política de roles de IAM para el bucket de S3
  - Política de roles de IAM para la clave de KMS
  - Política de roles de IAM para temas de Amazon SNS
  - Política de roles de IAM para obtener datos de configuración
  - Administración de permisos para el registro de buckets de S3

Creación de políticas de roles de IAM

Cuando utiliza la AWS Config consola para crear un rol de IAM, le asigna AWS Config automáticamente los permisos necesarios al rol.

Si lo utiliza AWS CLI para configurar AWS Config o actualizar un rol de IAM existente, debe actualizar manualmente la política para poder acceder AWS Config a su bucket de S3, publicar en su tema de SNS y obtener los detalles de configuración de sus recursos.

Adición de una política de confianza de IAM a su rol

Puede crear una política de confianza de IAM que le permita asumir una función y utilizarla AWS Config para realizar un seguimiento de sus recursos. Para obtener más información sobre las políticas de confianza, consulte Términos y conceptos de roles en la Guía del usuario de IAM.

El siguiente es un ejemplo de política de confianza para los AWS Config roles:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

Puede utilizar la condición `AWS:SourceAccount` de la relación de confianza del rol de IAM anterior para restringir que la entidad principal del servicio de Config solo interactúe con el rol de AWS IAM cuando realice operaciones en nombre de cuentas específicas.

AWS Config también admite la `AWS:SourceArn` condición que restringe al director del servicio Config a asumir únicamente la función de IAM cuando realiza operaciones en nombre de la cuenta propietaria. Cuando se utiliza la AWS Config entidad principal de servicio, la `AWS:SourceArn`

propiedad siempre se establece `arn:aws:config:sourceRegion:sourceAccountID:*` en `sourceRegion` la región del registrador de configuración gestionado por el cliente y `sourceAccountID` en el identificador de la cuenta que contiene el registrador de configuración gestionado por el cliente.

Por ejemplo, agregue la siguiente condición para hacer que la entidad principal del servicio Config solo asuma el rol de IAM en nombre de un registrador de configuración administrado por el cliente en la región `us-east-1` de la cuenta `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Política de roles de IAM para el bucket de S3

El siguiente ejemplo de política otorga AWS Config permiso para acceder a su bucket de S3:

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
```

```
}
```

Política de roles de IAM para la clave de KMS

El siguiente ejemplo de política otorga AWS Config permiso para usar el cifrado basado en KMS en nuevos objetos para la entrega de cubos en S3:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
        }
    ]
}
```

Política de roles de IAM para temas de Amazon SNS

El siguiente ejemplo de política otorga AWS Config permiso para acceder a tu tema de SNS:

JSON

```
{
  "Version":"2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"arn:aws:sns:us-east-1:123456789012:MyTopic"
     }
```

```
    ]
}
```

Si el tema de SNS se cifra para instrucciones adicionales sobre la configuración, consulte Configuración de los permisos de AWS KMS en la Guía para desarrolladores de Amazon Simple Notification Service.

Política de roles de IAM para obtener datos de configuración

Se recomienda utilizar el rol AWS Config vinculado al servicio:. `AWSServiceRoleForConfig` Los roles vinculados al servicio están predefinidos e incluyen todos los permisos necesarios para llamar a otros AWS Config . Servicios de AWS El rol AWS Config vinculado al servicio es obligatorio para los grabadores de configuración vinculados al servicio. Para obtener más información, consulte Uso de roles vinculados a servicios para AWS Config.

Si crea o actualiza un rol con la consola, AWS Config lo adjunta automáticamente. AWSServiceRoleForConfig

Si utiliza el AWS CLI, utilice el `attach-role-policy` comando y especifique el nombre de recurso de Amazon (ARN) para: AWSServiceRoleForConfig

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForConfig
```

Administración de permisos para el registro de buckets de S3

AWS Config registra y envía notificaciones cuando se crea, actualiza o elimina un bucket de S3.

Se recomienda utilizar el rol AWS Config vinculado al servicio:. `AWSServiceRoleForConfig` Los roles vinculados al servicio están predefinidos e incluyen todos los permisos necesarios para llamar a otros AWS Config . Servicios de AWS El rol AWS Config vinculado al servicio es obligatorio para los grabadores de configuración vinculados al servicio. Para obtener más información, consulte Uso de roles vinculados a servicios para AWS Config.

Actualización del rol de IAM para el registrador de configuración administrado por el cliente

Puede actualizar el rol de IAM utilizado por el registrador de configuración administrado por el cliente. Antes de actualizar el rol de IAM, asegúrese de haber creado un nuevo rol para sustituir al

anterior. Debe adjuntar políticas al nuevo rol que otorgan permisos AWS Config para registrar las configuraciones y entregarlas a su canal de entrega.

Para obtener información sobre cómo crear un rol de IAM y asociar las políticas necesarias al rol de IAM, consulte Paso 3: crear un rol de IAM.

> **Note**
>
> Para encontrar el ARN de un rol de IAM existente, vaya a la consola de IAM en. https://console.aws.amazon.com/iam/ Seleccione Roles en el panel de navegación. A continuación, elija el nombre del rol que desee y encuentre el ARN en la parte superior de la página Summary (Resumen).

Actualización del rol de IAM

Puede actualizar su función de IAM mediante el o el. Consola de administración de AWS AWS CLI

To update the IAM role (Console)

1. Inicie sesión en la AWS Config consola de su https://console.aws.amazon.com/config/casa Consola de administración de AWS y ábrala.
2. Seleccione Configuración en el panel de navegación.
3. En la pestaña Registrador administrado por el cliente, seleccione Editar en la página Configuración.
4. En la sección Gobernanza de datos, elija la función de IAM para AWS Config:
   - Usa un rol AWS Config vinculado a un servicio existente: AWS Config crea un rol que tenga los permisos necesarios.
   - Elegir un rol de su cuenta: para Roles existentes, seleccione un rol de IAM en su cuenta.
5. Seleccione Save.

To update the IAM role (AWS CLI)

Utilice el comando `put-configuration-recorder` y especifique el nombre de recurso de Amazon (ARN) del nuevo rol:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

Permisos del bucket de Amazon S3 para el canal AWS Config de entrega

> **Important**
>
> Esta página trata sobre cómo configurar el Amazon S3 Bucket para el canal AWS Config de entrega. Esta página no trata sobre el tipo `AWS::S3::Bucket` de recurso que puede grabar la grabadora de AWS Config configuración.

De forma predeterminada, los buckets y los objetos de Amazon S3 son privados. Solo la persona Cuenta de AWS que creó el depósito (el propietario del recurso) tiene permisos de acceso. Los propietarios de recursos pueden conceder acceso a otros recursos y usuarios creando políticas de acceso.

Cuando crea AWS Config automáticamente un bucket de S3 para usted, añade los permisos necesarios. No obstante, si especifica un bucket de S3 existente, debe agregar estos permisos de forma manual.

Temas

- Permisos necesarios para el bucket de Amazon S3 cuando se utilizan roles de IAM
- Permisos necesarios para el bucket de Amazon S3 cuando se utilizan roles vinculados a servicios
- Concesión de AWS Config acceso al Amazon S3 Bucket
- Permisos necesarios para el bucket de Amazon S3 cuando se realizan entregas entre cuentas

Permisos necesarios para el bucket de Amazon S3 cuando se utilizan roles de IAM

AWS Config utiliza la función de IAM que asignó al grabador de configuración para enviar el historial de configuración y las instantáneas a los depósitos de S3 de su cuenta. Para la entrega entre cuentas, AWS Config primero intenta usar la función de IAM asignada. Si la política de bucket no concede acceso a `WRITE` al rol de IAM, AWS Config utiliza la entidad principal de servicio `config.amazonaws.com`. La política de bucket debe conceder acceso a `WRITE` a `config.amazonaws.com` para completar la entrega. Tras una entrega correcta, AWS Config conserva la propiedad de todos los objetos que entrega al depósito S3 multicuenta.

AWS Config llama a la HeadBucketAPI de Amazon S3 con la función de IAM que asignó al registrador de configuración para confirmar si el bucket de S3 existe y su ubicación. Si no tiene los permisos necesarios AWS Config para confirmarlo, aparecerá un `AccessDenied` error en sus AWS CloudTrail registros. Sin embargo, AWS Config puede seguir proporcionando el historial de configuración y las instantáneas aunque AWS Config no disponga de los permisos necesarios para confirmar la existencia del bucket de S3 y su ubicación.

> **Permisos mínimos**
>
> La API `HeadBucket` de Amazon S3 requiere esta acción `s3:ListBucket`.

Permisos necesarios para el bucket de Amazon S3 cuando se utilizan roles vinculados a servicios

El rol AWS Config vinculado al servicio no tiene permiso para colocar objetos en los buckets de Amazon S3. Si lo configura AWS Config mediante un rol vinculado a un servicio, AWS Config utilizará el principal de `config.amazonaws.com` servicio para entregar el historial de configuración y las instantáneas. La política de compartimentos de S3 de su cuenta o de los destinos de varias cuentas debe incluir permisos para que el director del AWS Config servicio escriba objetos.

Concesión de AWS Config acceso al Amazon S3 Bucket

Complete los siguientes pasos AWS Config para enviar el historial de configuración y las instantáneas a un bucket de Amazon S3.

1. Inicie sesión Consola de administración de AWS con la cuenta que tiene el bucket de S3.
2. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
3. Seleccione el depósito que quiere usar AWS Config para entregar los elementos de configuración y, a continuación, elija Propiedades.
4. Elija Permisos.
5. Elija Edit Bucket Policy.
6. Copie la siguiente política en la ventana Bucket Policy Editor (Editor de política de bucket):

> **Prácticas recomendadas de seguridad**
>
> Le recomendamos encarecidamente que restrinja el acceso a la política de bucket con la condición `AWS:SourceAccount`. Esto garantiza que solo AWS Config se conceda el acceso en nombre de los usuarios esperados.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
```

```
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

7. Cambie los siguientes valores de la política del bucket:

   - *amzn-s3-demo-bucket*— Nombre del bucket de Amazon S3 donde se AWS Config entregarán el historial de configuración y las instantáneas.
   - *[optional] prefix*— Una adición opcional a la clave de objeto de Amazon S3 que ayuda a crear una organización similar a una carpeta en el bucket.
   - *sourceAccountID*— ID de la cuenta en la que se AWS Config entregarán el historial de configuración y las instantáneas.
8. Elija Save (Guardar) y, a continuación, Close (Cerrar).

La `AWS:SourceAccount` condición restringe las AWS Config operaciones a lo especificado. Cuentas de AWS Para las configuraciones de varias cuentas dentro de una organización que realizan entregas en un único segmento de S3, utilice funciones de IAM con claves de AWS Organizations condiciones en lugar de funciones vinculadas al servicio. Por ejemplo, `AWS:PrincipalOrgID`. Para obtener más información, consulte Administración de permisos de acceso para una organización en la Guía del usuario de AWS Organizations .

La `AWS:SourceArn` condición restringe las AWS Config operaciones a canales de entrega específicos. El formato de `AWS:SourceArn` es el siguiente: `arn:aws:config:`*`sourceRegion`*`:`*`123456789012`*.

Por ejemplo, para restringir el acceso al bucket de S3 a un canal de entrega en la región Este de EE. UU. (Norte de Virginia) de la cuenta 123456789012, añada la siguiente condición:

```
"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:"}
```

Permisos necesarios para el bucket de Amazon S3 cuando se realizan entregas entre cuentas

Si AWS Config está configurado para entregar el historial de configuración y las instantáneas a un bucket de Amazon S3 en una cuenta diferente (configuración multicuenta), donde el registrador de configuración y el bucket de S3 especificado para el canal de entrega son diferentes Cuentas de AWS, se requieren los siguientes permisos:

- El rol de IAM que asigne al registrador de configuración necesita un permiso explícito para realizar la operación `s3:ListBucket`. Esto se debe a que AWS Config llama a la HeadBucketAPI de Amazon S3 con esta función de IAM para determinar la ubicación del bucket.
- La política de bucket de S3 debe incluir los permisos para la función de IAM asignada al registrador de configuración.

A continuación se muestra un ejemplo de política de bucket.

```
{
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IAM Role-Arn assigned to the configuration recorder"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
}
```

Permisos para la clave KMS del canal de AWS Config entrega

Utilice la información de este tema si desea crear una política para una AWS KMS clave para su depósito de S3 que le permita utilizar el cifrado basado en KMS en los objetos entregados AWS Config por el depósito de S3.

Contenido

- Permisos necesarios para la clave de KMS si se utilizan roles de IAM (entrega de buckets de S3)
- Permisos necesarios para la AWS KMS clave cuando se utilizan funciones vinculadas al servicio (S3 Bucket Delivery)
- Otorgar AWS Config acceso a la AWS KMS clave

Permisos necesarios para la clave de KMS si se utilizan roles de IAM (entrega de buckets de S3)

Si lo configuras AWS Config con un rol de IAM, puedes adjuntar la siguiente política de permisos a la clave de KMS:

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> Si el rol de IAM, la política del bucket de Amazon S3 o la AWS KMS clave no proporcionan el acceso adecuado AWS Config, se producirá AWS Config un error al intentar enviar la información de configuración al bucket de Amazon S3. En este caso, vuelve AWS Config a enviar la información, esta vez como principal del AWS Config servicio. En este caso,

debe adjuntar una política de permisos, que se menciona a continuación, a la AWS KMS clave para permitir el AWS Config acceso y usarla cuando entregue información al bucket de Amazon S3.

Permisos necesarios para la AWS KMS clave cuando se utilizan funciones vinculadas al servicio (S3 Bucket Delivery)

El rol AWS Config vinculado al servicio no tiene permiso para acceder a la clave. AWS KMS Por lo tanto, si lo configuras AWS Config con un rol vinculado al servicio, AWS Config enviará la información como responsable del AWS Config servicio. Deberá adjuntar una política de acceso, que se menciona a continuación, a la AWS KMS clave para conceder el AWS Config acceso y poder AWS KMS utilizarla cuando entregue información al bucket de Amazon S3.

Otorgar AWS Config acceso a la AWS KMS clave

Esta política permite AWS Config utilizar una AWS KMS clave al entregar información a un bucket de Amazon S3.

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

Cambie los siguientes valores de la política de claves:

- *myKMSKeyARN*— El ARN de la AWS KMS clave utilizada para cifrar los datos del bucket de Amazon S3 al que se AWS Config entregarán los elementos de configuración a.
- *sourceAccountID*— El ID de la cuenta a la que se AWS Config entregarán los elementos de configuración.

Puedes usar la `AWS:SourceAccount` condición de la política AWS KMS clave anterior para restringir que el director del servicio Config solo interactúe con la AWS KMS clave cuando realice operaciones en nombre de cuentas específicas.

AWS Config también admite la `AWS:SourceArn` condición que restringe al director del servicio Config a interactuar únicamente con el bucket de Amazon S3 cuando realiza operaciones en nombre de canales de AWS Config entrega específicos. Al usar el AWS Config servicio principal, la `AWS:SourceArn` propiedad siempre estará configurada `arn:aws:config:sourceRegion:sourceAccountID:*` en `sourceRegion` la región del canal de entrega y `sourceAccountID` en el ID de la cuenta que contiene el canal de entrega. Para obtener más información sobre los canales de AWS Config entrega, consulte Administración del canal de entrega. Por ejemplo, añada la siguiente condición para restringir que la entidad principal del servicio de Config interactúe con su bucket de Amazon S3 únicamente en nombre de un canal de entrega de la región `us-east-1` de la cuenta `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Permisos para el tema de Amazon SNS

> **No se admite Amazon SNS cifrado**
>
> AWS Config no admite temas cifrados de Amazon SNS.

En este tema se describe cómo configurar AWS Config para entregar temas de Amazon SNS que pertenecen a una cuenta diferente. AWS Config debe tener los permisos necesarios para enviar notificaciones a un tema de Amazon SNS.

Cuando la AWS Config consola cree un tema nuevo de Amazon SNS para usted, le AWS Config concede los permisos necesarios. Si elige un tema de Amazon SNS existente, asegúrese de que el tema de Amazon SNS incluya los permisos necesarios y siga las prácticas recomendadas de seguridad.

> **No se admiten temas de Amazon SNS entre regiones**
>
> AWS Config actualmente solo admite el acceso dentro de la misma cuenta Región de AWS y entre cuentas.

Contenido

- Permisos necesarios para el tema de Amazon SNS cuando se utilizan roles de IAM
- Permisos necesarios para el tema de Amazon SNS cuando se utilizan roles vinculados a servicios
- Concesión de AWS Config acceso al tema Amazon SNS
- Solución de problemas del tema de Amazon SNS

Permisos necesarios para el tema de Amazon SNS cuando se utilizan roles de IAM

Puede asociar una política de permisos al tema de Amazon SNS propiedad de una cuenta diferente. Si desea utilizar un tema de Amazon SNS de otra cuenta, asegúrese de asociar la siguiente política a un tema de Amazon SNS existente.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

Para la `Resource` clave, *`account-id`* es el número de AWS cuenta del propietario del tema. Para*`account-id1`*, y *`account-id2account-id3`*, usa el tema Cuentas de AWS que enviará datos a un tema de Amazon SNS. Puede sustituir los valores adecuados por *`region`* y*`myTopic`*.

Cuando AWS Config envía una notificación a un tema de Amazon SNS, primero intenta usar el rol de IAM, pero este intento falla si el rol o Cuenta de AWS no tiene permiso para publicar en el tema. En este caso, vuelve AWS Config a enviar la notificación, esta vez como un nombre principal de AWS Config servicio (SPN). Para que la entrega se realice correctamente, la política de acceso del tema debe conceder a `sns:Publish` acceso al nombre de la entidad principal de `config.amazonaws.com`. Debe asociar una política de acceso, que se describe en la siguiente sección, al tema de Amazon SNS para conceder a AWS Config acceso al tema de Amazon SNS si el rol de IAM no tiene permiso para publicar en el tema.

Permisos necesarios para el tema de Amazon SNS cuando se utilizan roles vinculados a servicios

El rol AWS Config vinculado al servicio no tiene permiso para acceder al tema de Amazon SNS. Por lo tanto, si lo configuras AWS Config mediante un rol vinculado a un servicio (SLR), en su lugar AWS Config enviará la información como responsable del servicio. AWS Config Deberá adjuntar una política de acceso, que se menciona a continuación, al tema Amazon SNS para permitir el AWS Config acceso y enviar información al tema Amazon SNS.

Para configurar en la misma cuenta, si el tema de Amazon SNS y el SLR están en la misma cuenta y la política de Amazon SNS concede el permiso `sns:Publish` al SLR, no será necesario utilizar el SPN de AWS Config . La siguiente política de permisos y las prácticas recomendadas de seguridad se refieren a la configuración en varias cuentas.

Concesión de AWS Config acceso al tema Amazon SNS

Esta política permite AWS Config enviar una notificación a un tema de Amazon SNS. Para conceder AWS Config acceso al tema de Amazon SNS desde otra cuenta, tendrás que adjuntar la siguiente política de permisos.

> **Note**
>
> Como práctica recomendada de seguridad, se recomienda encarecidamente asegurarse de que solo AWS Config se accede a los recursos en nombre de los usuarios esperados restringiendo el acceso a las cuentas que figuran en esa `AWS:SourceAccount` condición.

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

Para la `Resource` clave, *`account-id`* es el número de AWS cuenta del propietario del tema. Para*`account-id1`*, y *`account-id2account-id3`*, usa el tema Cuentas de AWS que enviará datos a un tema de Amazon SNS. Puede sustituir los valores adecuados por *`region`* y*`myTopic`*.

Puede utilizar la `AWS:SourceAccount` condición de la política de temas anterior de Amazon SNS para restringir el nombre principal del AWS Config servicio (SPN) para que solo interactúe con el tema de Amazon SNS cuando realice operaciones en nombre de cuentas específicas.

AWS Config también admite la `AWS:SourceArn` condición que restringe el nombre principal del AWS Config servicio (SPN) a interactuar únicamente con el bucket de S3 cuando se realizan operaciones en nombre de canales de entrega específicos. AWS Config Si se utiliza el nombre principal del AWS Config servicio (SPN), la `AWS:SourceArn` propiedad siempre se establece `arn:aws:config:sourceRegion:sourceAccountID:*` en `sourceRegion` la región del canal de entrega y `sourceAccountID` en el identificador de la cuenta que contiene el canal de entrega. Para obtener más información sobre los canales AWS Config de entrega, consulte Administración del canal de entrega. Por ejemplo, añada la siguiente condición para restringir que el nombre principal del AWS Config servicio (SPN) interactúe con su bucket de S3 únicamente en

nombre de un canal de entrega de la `us-east-1` región de la cuenta`123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`

Solución de problemas del tema de Amazon SNS

AWS Config debe tener permisos para enviar notificaciones a un tema de Amazon SNS. Si un tema de Amazon SNS no puede recibir notificaciones, compruebe que la función de IAM que AWS Config estaba asumiendo tiene los permisos necesarios. `sns:Publish`

Solución de problemas de AWS Config identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con un AWS Config IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AWS Config
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Config recursos

No estoy autorizado a realizar ninguna acción en AWS Config

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `config:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

En este caso, la política de Mateo se debe actualizar para permitirle acceder al recurso *`my-example-widget`* mediante la acción `config:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS Config.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Config. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Config recursos

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS Config es compatible con estas funciones, consulte. ¿Cómo AWS Config funciona con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de funciones vinculadas a servicios para AWS Config

AWS Config utiliza funciones AWS Identity and Access Management vinculadas al servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Config Los roles vinculados al servicio están predefinidos AWS Config e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Config , ya que no es necesario añadir manualmente los permisos necesarios. AWS Config define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Config puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service Linked Role (Rol vinculado a servicios). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados al servicio para AWS Config

AWS Config usa el rol vinculado al servicio denominado AwsServiceRoleForConfig: AWS Config usa este rol vinculado al servicio para llamar a otros servicios en su nombre. AWS Para ver las actualizaciones más recientes, consulte the section called “Actualizaciones de políticas”.

El rol vinculado a servicios AwsServiceRoleForConfig confía en el servicio `config.amazonaws.com` para asumir el rol.

La política de permisos del `AwsServiceRoleForConfig` rol contiene permisos de solo lectura y solo escritura para los recursos y permisos de solo lectura para AWS Config los recursos de

otros servicios compatibles. AWS Config Para ver la política administrada de, consulte Políticas administradas de AwsServiceRoleForConfig.AWSAWS Config

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Para utilizar un rol vinculado a un servicio AWS Config, debe configurar los permisos en su bucket de Amazon S3 y en el tema de Amazon SNS. Para obtener más información, consulte Permisos necesarios para el bucket de Amazon S3 cuando se utilizan roles vinculados a servicios, Permisos necesarios para la AWS KMS clave cuando se utilizan funciones vinculadas al servicio (S3 Bucket Delivery) y Permisos necesarios para el tema de Amazon SNS cuando se utilizan roles vinculados a servicios.

Crear un rol vinculado a un servicio para AWS Config

En la CLI de IAM o la API de IAM, cree un rol vinculado a servicio con el nombre de servicio `config.amazonaws.com`. Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado a un servicio para AWS Config

AWS Config no permite editar el rol vinculado al AwsServiceRoleForConfigservicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Edición de un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para AWS Config

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el AWS Config servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar AWS Config los recursos utilizados por el AwsServiceRoleForConfig

Compruebe que no haya `ConfigurationRecorders` que estén utilizando el rol vinculado al servicio. Puede utilizar la AWS Config consola para detener la grabadora de configuración. Para detener la grabación, en Recording is on (La grabación está activada), elija Turn off (Desactivar).

Puede eliminar la AWS Config API `ConfigurationRecorder` de uso. Para eliminarlo, utilice el comando`delete-configuration-recorder`.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado a servicios AwsServiceRoleForConfig. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Respuesta a incidentes en AWS Config

La seguridad de AWS es nuestra mayor prioridad. Como parte del modelo de responsabilidad compartida AWS en la nube, AWS administra un centro de datos, una red y una arquitectura de software que cumplen con los requisitos de las organizaciones más sensibles a la seguridad. AWS es responsable de cualquier respuesta a un incidente relacionado con el propio AWS Config servicio. Además, como AWS cliente, usted comparte la responsabilidad de mantener la seguridad en la nube. Esto significa que usted controla la seguridad que decide implementar desde las AWS herramientas y funciones a las que tiene acceso, y es responsable de la respuesta a los incidentes, según su parte del modelo de responsabilidad compartida.

Al establecer una base de seguridad que cumpla con los objetivos de las aplicaciones que se ejecutan en la nube, puede detectar las desviaciones a las que puede responder. Dado que la respuesta a los incidentes de seguridad puede ser un tema complejo, le recomendamos que consulte los siguientes recursos para que pueda comprender mejor el impacto que la respuesta a incidentes (IR) y sus elecciones tienen en sus objetivos corporativos: la Guía de respuesta a incidentes de AWS seguridad, el documento técnico sobre las mejores prácticas de AWS seguridad y el documento técnico sobre la perspectiva de seguridad del marco de adopción de la AWS nube (CAF).

Validación de la conformidad para AWS Config

Los auditores externos evalúan la seguridad y el cumplimiento AWS Config como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance by Compliance Servicios de AWS y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte AWS la documentación de seguridad.

Resiliencia en AWS Config

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Config

Como servicio gestionado, AWS Config está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Config través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Configuración y análisis de vulnerabilidades

Para AWS Config, se AWS encarga de las tareas de seguridad básicas, como la aplicación de parches al sistema operativo (SO) huésped y a las bases de datos, la configuración del firewall y la recuperación ante desastres.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puedes manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición `aws:SourceAccount`global `aws:SourceArn`y las claves de contexto en las políticas de recursos para limitar los permisos que se AWS Config otorgan a otro servicio al recurso. Utiliza `aws:SourceArn` si desea que solo se

asocie un recurso al acceso entre servicios. Utiliza `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con caracteres comodines (`*`) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:servicename:*:123456789012:*`.

Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos.

El siguiente ejemplo muestra cómo puede utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves de contexto AWS Config para evitar el confuso problema de los adjuntos: conceder AWS Config acceso al bucket de Amazon S3.

Mejores prácticas de seguridad para AWS Config

AWS Config proporciona una serie de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

- Aproveche el etiquetado para AWS Config facilitar la administración, la búsqueda y el filtrado de los recursos.
- Confirme que sus canales de entrega se hayan configurado correctamente y, una vez confirmados, compruebe que AWS Config se están grabando correctamente.

Para obtener más información, consulte la publicación del blog AWS Config best practices

Inicio de sesión y supervisión AWS Config

AWS Config está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Config. La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Config sus AWS soluciones.

Temas

- Registrar las llamadas a la AWS Config API con AWS CloudTrail
- Supervisión

Registrar las llamadas a la AWS Config API con AWS CloudTrail

CloudTrail captura todas las llamadas a la API AWS Config como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Config consola y llamadas en código a las operaciones de la AWS Config API. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Config. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar el destinatario de la solicitud AWS Config, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Temas

- AWS Config Información en CloudTrail
- Descripción de las entradas de los archivos de AWS Config registro
- Ejemplos de archivos de registro

AWS Config Información en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS Config, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su

Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos para AWS Config ti, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas AWS Config las operaciones se registran CloudTrail y se documentan en la referencia de la AWS Config API. Por ejemplo, las llamadas a las DeliverConfigSnapshotDescribeDeliveryChannelsoperaciones y y generan entradas en los archivos de CloudTrail registro. DeleteDeliveryChannel

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail .

Descripción de las entradas de los archivos de AWS Config registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Ejemplos de archivos de registro

Para ver ejemplos de las entradas de CloudTrail registro, consulta los siguientes temas.

DeleteDeliveryChannel

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la DeleteDeliveryChanneloperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
```

```
    }
```

DeliverConfigSnapshot

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la DeliverConfigSnapshotoperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
```

```
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

DescribeConfigurationRecorderStatus

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la DescribeConfigurationRecorderStatusoperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la DescribeConfigurationRecordersoperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la DescribeDeliveryChannelsoperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
```

```
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la GetResourceConfigHistoryoperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
```

```
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```

PutConfigurationRecorder

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la PutConfigurationRecorderoperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la PutDeliveryChanneloperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la StartConfigurationRecorderoperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

A continuación se muestra un ejemplo de archivo de CloudTrail registro de la StopConfigurationRecorderoperación.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
```

```
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

Supervisión

Puede utilizar otros AWS servicios para supervisar AWS Config los recursos.

- Puedes usar Amazon Simple Notification Service (SNS) para enviarte notificaciones cada vez que se cree, actualice o modifique un AWS recurso compatible como resultado de la actividad de la API del usuario.
- Puedes usar Amazon EventBridge para detectar cambios en el estado de los AWS Config eventos y reaccionar ante ellos.

Temas

- Supervisión de los cambios en los AWS recursos con Amazon SQS
- Monitorización AWS Config con Amazon EventBridge

Supervisión de los cambios en los AWS recursos con Amazon SQS

AWS Config utiliza Amazon Simple Notification Service (SNS) para enviarle notificaciones cada vez que se crea, actualiza o modifica un AWS recurso compatible como resultado de la actividad de la API del usuario. Sin embargo, es posible que solo le interesen determinados cambios en la configuración de los recursos. Por ejemplo, puede que considere esencial saber si alguien modifica la configuración de un grupo de seguridad, pero no necesita que se le informe cada vez que se produzca un cambio en las etiquetas de las instancias de Amazon EC2. O es posible que desee escribir un programa que realice acciones específicas cuando se actualizan recursos concretos. Por ejemplo, puede que desee iniciar un flujo de trabajo determinado cuando cambie la configuración de un grupo de seguridad. Si desea consumir los datos de forma programática de AWS Config

estas u otras formas, utilice una cola de Amazon Simple Queue Service como punto de enlace de notificación para Amazon SNS.

> **Note**
>
> Las notificaciones también pueden proceder de Amazon SNS en forma de correo electrónico, un SMS (servicio de mensajes cortos) para teléfonos móviles y smartphones que admiten SMS, un mensaje de notificación a una aplicación en un dispositivo móvil o un mensaje de notificación a uno o más puntos de conexión HTTP o HTTPS.

Puede tener una única cola de SQS para suscribirse a varios temas, tanto si dispone de un tema por región como un tema por cada cuenta y región. Debe suscribir la cola al tema de SNS que desee. (Puede suscribir varias colas a un tema de SNS). Para obtener más información, consulte Colas de distribución ramificada a Amazon SQS.

Permisos para Amazon SQS

Para usar Amazon SQS con AWS Config, debe configurar una política que conceda permisos a su cuenta para realizar todas las acciones permitidas en una cola de SQS. La siguiente política de ejemplo concede al número de cuenta 111122223333 y al número de cuenta 444455556666 permiso para enviar mensajes sobre cada cambio de configuración a la cola arn:aws:sqs:us-east-2:444455556666:queue1.

JSON

```
{
  "Version":"2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
```

```
}
```

También debe crear una política que conceda permisos de conexión entre un tema de SNS y la cola SQS que se suscribe a ese tema. El siguiente es un ejemplo de política que permite al tema de SNS con el nombre de recurso de Amazon (ARN) arn:aws:sns:us-east- 2:111122223333:test-topic realizar cualquier acción en la cola denominada arn:aws:sqs:us-east- 2:111122223333:. test-topic-queue

> **Note**
>
> La cuenta para el tema de SNS y la cola de SQS deben estar en la misma región.

JSON

```
{
  "Version":"2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

Cada política puede incluir instrucciones que abarquen una sola cola, no varias. Para obtener información sobre otras restricciones en las políticas de Amazon SQS, consulte Información especial sobre políticas de Amazon SQS.

Monitorización AWS Config con Amazon EventBridge

Amazon EventBridge ofrece un flujo casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. Usa Amazon EventBridge para detectar los cambios en el estado de los AWS Config eventos y reaccionar ante ellos.

Tiene la opción de crear una regla que se ejecute siempre que haya una transición de estado o cuando haya una transición a uno o varios estados de interés. A continuación, en función de las reglas que crees, Amazon EventBridge invoca una o más acciones de destino cuando un evento coincide con los valores que especificas en una regla. Dependiendo del tipo de evento, es posible que desee enviar notificaciones, capturar información sobre el evento, tomar medidas correctivas, iniciar eventos o adoptar otras acciones.

Sin embargo AWS Config, antes de crear las reglas de un evento, debe hacer lo siguiente:

- Familiarícese con los eventos, las reglas y los objetivos en EventBridge. Para obtener más información, consulta ¿Qué es Amazon EventBridge?
- Para obtener más información sobre cómo empezar a utilizar las reglas EventBridge y configurarlas, consulta Cómo empezar con Amazon EventBridge.
- Crear el destino o los destinos que se utilizarán en las reglas de eventos.

Temas

- Consideraciones
- EventBridge Formato de Amazon para AWS Config
- Creación de Amazon EventBridge Rule para AWS Config

Consideraciones

No recibirás alertas de EventBridge los siguientes tipos de recursos si no las estás grabando con AWS Config:

- `AWS::ACM::Certificate`
- `AWS::CloudTrail::Trail`
- `AWS::CloudWatch::Alarm`
- `AWS::EC2::CustomerGateway`
- `AWS::EC2::EIP`

- AWS::EC2::Host
- AWS::EC2::Instance
- AWS::EC2::InternetGateway
- AWS::EC2::NetworkAcl
- AWS::EC2::NetworkInterface
- AWS::EC2::RouteTable
- AWS::EC2::SecurityGroup
- AWS::EC2::Subnet
- AWS::EC2::VPC
- AWS::EC2::VPNConnection
- AWS::EC2::VPNGateway
- AWS::EC2::Volume
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::IAM::Group
- AWS::IAM::Policy
- AWS::IAM::Role
- AWS::IAM::User
- AWS::RDS::DBInstance
- AWS::RDS::DBSecurityGroup
- AWS::RDS::DBSnapshot
- AWS::RDS::DBSubnetGroup
- AWS::RDS::EventSubscription
- AWS::Redshift::Cluster
- AWS::Redshift::ClusterParameterGroup
- AWS::Redshift::ClusterSecurityGroup
- AWS::Redshift::ClusterSnapshot
- AWS::Redshift::ClusterSubnetGroup
- AWS::Redshift::EventSubscription
- AWS::S3::Bucket

EventBridge Formato de Amazon para AWS Config

El formato del EventBridge AWS Config evento es el siguiente:

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

Creación de Amazon EventBridge Rule para AWS Config

Siga los siguientes pasos para crear una EventBridge regla que se active en función de un evento emitido por AWS Config. Los eventos se emiten en la medida de lo posible.

1. En el panel de navegación, seleccione Reglas.
2. Elija Creación de regla.
3. Escriba un nombre y una descripción para la regla.

   Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

   > **Note**
   >
   > Un bus de eventos recibe eventos de una fuente, usa reglas para evaluarlos, aplica cualquier transformación de entrada configurada y los enruta a los destinos adecuados. El bus de eventos predeterminado de su cuenta recibe eventos de Servicios de AWS. Un bus de eventos personalizado puede recibir eventos de sus aplicaciones y servicios

personalizados. Un bus de eventos asociado recibe eventos de una fuente de eventos creada por un socio de SaaS. Estos eventos provienen de los servicios o aplicaciones de socios. Para obtener más información, consulta los autobuses de eventos en Amazon EventBridge en la Guía del EventBridge usuario de Amazon.

4. En Tipo de regla, elija Regla con un patrón de evento.
5. En Origen del evento, selecciona AWS eventos o eventos EventBridge asociados.
6. (Opcional) En Ejemplo de tipo de evento, elija Eventos de AWS .
7. (Opcional) En Tipo de evento, elija el tipo de evento que activará la regla:
   - Seleccione Llamar a la AWS API desde CloudTrail para basar las reglas en las llamadas a la API realizadas a este servicio. Para obtener más información sobre la creación de este tipo de regla, consulta el Tutorial: Crear una EventBridge regla de Amazon para llamadas a la AWS CloudTrail API.
   - Elija Config Configuration Item Change (Config: Cambio de un elemento de configuración) para recibir notificaciones cuando cambie un recurso de su cuenta.

     Como se describe en estos artículos de soporte, puedes utilizarlos EventBridge para recibir notificaciones personalizadas por correo electrónico cuando se crea o se elimina un recurso. ¿Cómo puedo recibir notificaciones por correo electrónico personalizadas cuando se crea un recurso en el AWS Config servicio que Cuenta de AWS uso? y ¿cómo puedo recibir notificaciones por correo electrónico personalizadas cuando se elimina un recurso del AWS Config servicio que Cuenta de AWS uso? .
   - Elija Config Rules Compliance Change (Config: Cambio en la conformidad de las reglas) para obtener notificaciones cuando se produzca un error en una comprobación de conformidad de sus reglas.

     Como se describe en este artículo de soporte, puede utilizarlos EventBridge para recibir notificaciones personalizadas por correo electrónico cuando un recurso no es compatible. ¿Cómo puedo recibir una notificación cuando un AWS recurso no es compatible con el uso? AWS Config.
   - Elija Config Rules Re-evaluation Status (Config: Estado de reevaluación de reglas) para obtener notificaciones de estado de reevaluación.
   - Elija Config Configuration Snapshot Delivery Status (Config: Estado de entrega de instantáneas de configuración) para obtener notificaciones de estado de entrega de instantáneas de configuración.

- Elija Config Configuration History Delivery Status (Config: Estado de entrega del historial de configuración) para obtener notificaciones de estado de entrega del historial de configuración.

8. En Método de creación, elija Uso de forma de patrón.
9. En Origen de evento, seleccione Servicios de AWS .
10. Para el Servicio de AWS , seleccione Config.
11. En Tipo de evento, elija el tipo de evento que activará la regla:

- Selecciona Todos los eventos para establecer una regla que se aplique a todos los AWS servicios. Si elige esta opción, no podrá elegir tipos de mensajes, nombres de reglas, tipos de recursos o recursos específicos IDs.
- Seleccione Llamar a la AWS API desde CloudTrail para basar las reglas en las llamadas a la API realizadas a este servicio. Para obtener más información sobre la creación de este tipo de regla, consulta el Tutorial: Crear una EventBridge regla de Amazon para llamadas a la AWS CloudTrail API.
- Elija Config Configuration Item Change (Config: Cambio de un elemento de configuración) para recibir notificaciones cuando cambie un recurso de su cuenta.

  Como se describe en estos artículos de soporte, puedes utilizarlos EventBridge para recibir notificaciones personalizadas por correo electrónico cuando se crea o se elimina un recurso. ¿Cómo puedo recibir notificaciones por correo electrónico personalizadas cuando se crea un recurso en el AWS Config servicio que Cuenta de AWS uso? y ¿cómo puedo recibir notificaciones por correo electrónico personalizadas cuando se elimina un recurso del AWS Config servicio que Cuenta de AWS uso? .
- Elija Config Rules Compliance Change (Config: Cambio en la conformidad de las reglas) para obtener notificaciones cuando se produzca un error en una comprobación de conformidad de sus reglas.

  Como se describe en este artículo de soporte, puede utilizarlos EventBridge para recibir notificaciones personalizadas por correo electrónico cuando un recurso no es compatible. ¿Cómo puedo recibir una notificación cuando un AWS recurso no es compatible con el uso? AWS Config.
- Elija Config Rules Re-evaluation Status (Config: Estado de reevaluación de reglas) para obtener notificaciones de estado de reevaluación.
- Elija Config Configuration Snapshot Delivery Status (Config: Estado de entrega de instantáneas de configuración) para obtener notificaciones de estado de entrega de instantáneas de configuración.

- Elija Config Configuration History Delivery Status (Config: Estado de entrega del historial de configuración) para obtener notificaciones de estado de entrega del historial de configuración.

12. Elija Any message type (Cualquier tipo de mensaje) para recibir notificaciones de cualquier tipo. Elija Specific message type(s) (Tipos de mensajes específicos) para recibir los siguientes tipos de notificaciones:
    - Si lo desea ConfigurationItemChangeNotification, recibirá mensajes cuando cambie la configuración de un recurso que AWS Config evalúa.
    - Si lo desea ComplianceChangeNotification, recibirá mensajes cuando cambie el tipo de conformidad de un recurso que AWS Config evalúa.
    - Si lo desea ConfigRulesEvaluationStarted, recibirá mensajes cuando AWS Config comience a evaluar la regla con respecto a los recursos especificados.
    - Si lo desea ConfigurationSnapshotDeliveryCompleted, recibirá mensajes cuando entregue AWS Config correctamente la instantánea de configuración a su bucket de Amazon S3.
    - Si lo desea ConfigurationSnapshotDeliveryFailed, recibirá mensajes cuando AWS Config no pueda entregar la instantánea de configuración a su bucket de Amazon S3.
    - Si lo desea ConfigurationSnapshotDeliveryStarted, recibirá mensajes cuando AWS Config comience a entregar la instantánea de configuración a su bucket de Amazon S3.
    - Si lo desea ConfigurationHistoryDeliveryCompleted, recibirá mensajes cuando entregue AWS Config correctamente el historial de configuración a su bucket de Amazon S3.
13. Si eligió un tipo de evento específico de la lista desplegable Tipo de evento, elija Cualquier tipo de recurso para crear una regla que se aplique a todos los tipos de recursos AWS Config compatibles.

    O elija Specific resource type(s) (Tipos de recursos específicos) y, a continuación, escriba el tipo de recurso admitido por AWS Config (por ejemplo, `AWS::EC2::Instance`).
14. Si ha elegido un tipo de evento específico en la lista desplegable Tipo de evento, elija Cualquier ID de recurso para incluir cualquier ID de recurso admitido por AWS Config .

    O elija Specific resource ID(s) (ID de recursos específicos) y, a continuación, escriba el ID de recurso admitido por AWS Config (por ejemplo, `i-04606de676e635647`).
15. Si ha elegido un tipo de evento específico en la lista desplegable Tipo de evento, elija Cualquier nombre de regla para incluir cualquier regla admitida por AWS Config .

    O elija Specific rule name(s) (Nombres de reglas específicas) y, a continuación, escriba la regla admitida por AWS Config (por ejemplo, required-tags).

16. En la lista Seleccionar destinos, elija el tipo de destino definido para usar con esta regla y luego configure las opciones adicionales que requiera dicho tipo.
17. Los campos mostrados varían en función del servicio que seleccione. Introduzca la información específica de este tipo de destino, según sea necesario.
18. Para muchos tipos de objetivos, EventBridge necesita permisos para enviar eventos al destino. En estos casos, EventBridge puede crear la función de IAM necesaria para que se ejecute la regla.
    - Para crear un rol de IAM automáticamente, elija Creación de un nuevo rol para este recurso específico.
    - Para utilizar un rol de IAM que haya creado antes, elija Use existing role (Usar rol existente).
19. (Opcional) Elija Add target (Añadir destino) para añadir otro destino para esta regla.
20. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulta las EventBridge etiquetas de Amazon.
21. Revise la configuración de las reglas para asegurarse de que se ajusta a los requisitos de monitorización de eventos.
22. Elija Crear para confirmar la opción elegida.

Uso de AWS Config con los puntos de conexión de interfaz de Amazon VPC

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar sus recursos de AWS, puede establecer una conexión privada entre su VPC y AWS Config. Puede utilizar esta conexión para comunicarse con AWS Config desde su VPC sin pasar por la Internet pública.

Amazon VPC es un servicio de AWS que puede utilizar para lanzar recursos de AWS en una red virtual que defina. Con una VPC, puede controlar la configuración de la red, como el rango de direcciones IP, las subredes, las tablas de ruteo y las gateways de red. Los puntos de conexión de VPC de tipo interfaz utilizan la tecnología de AWSPrivateLink, una tecnología de AWS que permite la comunicación privada entre los servicios de AWS mediante una interfaz de red elástica con direcciones IP privadas. Para conectar su VPC a AWS Config, debe definir un punto de enlace de la VPC de tipo interfaz para AWS Config. Este tipo de punto de enlace le permite conectar la VPC a los servicios de AWS. El punto de enlace ofrece conectividad escalable de confianza con AWS Config sin necesidad de utilizar una gateway de Internet, una instancia de conversión de las direcciones de red (NAT) o una conexión de VPN. Para obtener más información, consulte Qué es Amazon VPC en la Guía del usuario de Amazon VPC.

Los siguientes pasos son para usuarios de Amazon VPC. Para obtener más información, consulte Introducción en la Guía del usuario de Amazon VPC.

Creación de un punto de conexión de VPC para AWS Config

Para comenzar a utilizar AWS Config con su VPC, cree un punto de enlace de la VPC de tipo interfaz para AWS Config. No es necesario cambiar la configuración de AWS Config. AWS Config llama a otros servicios de AWS con sus puntos de enlace públicos. Para obtener más información, consulte Creación de un punto de conexión de tipo interfaz en la Guía del usuario de Amazon VPC.

Preguntas frecuentes

No puedo ver los últimos cambios de configuración

¿Debería poder ver los cambios de configuración de inmediato?

AWS Config normalmente registra los cambios de configuración de los recursos inmediatamente después de detectar un cambio o con la frecuencia que usted especifique. Aunque el sistema hace todo lo posible porque sea así, a veces puede tardar más tiempo. Si los problemas persisten después de un tiempo, ponte en contacto con Amazon Soporte y proporciona tus AWS Config estadísticas compatibles CloudWatch. Para obtener más información sobre estas métricas, consulte AWS Config Usage and Success Metrics.

Relaciones indirectas en AWS Config

Temas

- ¿Qué es una relación de recursos?
- ¿Qué es una relación directa e indirecta con respecto a un recurso?
- ¿Qué relaciones indirectas AWS Config admite?
- ¿Qué escenarios utilizan relación indirecta?
- ¿Cómo se crean los elementos de configuración según la relación directa e indirecta?
- ¿Cuáles son los elementos de configuración que se generan por las relaciones indirectas?
- ¿Cómo deshabilito la relación indirecta?
- ¿Cómo puedo obtener los datos de configuración vinculados con las relaciones indirectas?

¿Qué es una relación de recursos?

En AWS, los recursos se refieren a entidades que se pueden administrar, como una instancia de Amazon Elastic Compute Cloud (Amazon EC2), una AWS CloudFormation pila o un bucket de Amazon S3. AWS Config es un servicio que rastrea y monitorea los recursos mediante la creación de elementos de configuración (CIs) cada vez que se detecta un cambio en un tipo de recurso registrado, o con la frecuencia de grabación que usted establezca. Por ejemplo, cuando AWS Config se configura para realizar un seguimiento de las instancias de Amazon EC2, crea un

elemento de configuración cada vez que se crea, actualiza o elimina una instancia. Cada elemento de configuración creado por AWS Config tiene varios campos, entre los que se incluyen`accountId`, `arn` (Nombre del recurso de Amazon) `awsRegionconfiguration`,`tags`,, `yrelationships`. El campo de relaciones de un CI permite AWS Config mostrar cómo se vinculan los recursos entre sí. Por ejemplo, una relación puede indicar que un volumen de Amazon EBS con el ID `vol-123ab45d` está asociado a una instancia de Amazon EC2 con el ID `i-a1b2c3d4`, que está asociado al grupo de seguridad `sg-ef678hk`.

¿Qué es una relación directa e indirecta con respecto a un recurso?

AWS Config deriva las relaciones de la mayoría de los tipos de recursos del campo de configuración, que se denominan relaciones «directas». Una relación directa es una conexión unidireccional (A→B) entre un recurso (A) y otro recurso (B), que normalmente se obtiene a partir de la respuesta descrita por la API del recurso (A). En el pasado, para algunos tipos de recursos que AWS Config inicialmente eran compatibles, también capturaba las relaciones de las configuraciones de otros recursos, creando relaciones «indirectas» que eran bidireccionales (B→A). Por ejemplo, la relación entre una instancia de Amazon EC2 y su grupo de seguridad es directa porque los grupos de seguridad se incluyen en la respuesta descrita por la API para la instancia de Amazon EC2. Por otro lado, la relación entre un grupo de seguridad y una instancia de Amazon EC2 es indirecta porque la descripción de un grupo de seguridad no devuelve información sobre las instancias a las que está asociado.

Por ejemplo, las relaciones indirectas pueden ayudar a responder a las preguntas siguientes:

- Cuando falla una puerta de enlace NAT, ¿qué instancias de EC2 de las subredes privadas se ven afectadas?
- Si se modifica una tabla de enrutamiento, ¿qué instancia de EC2 podría tener problemas de conectividad?
- ¿Qué grupo de seguridad no se ha utilizado nunca?
- ¿Qué ENI secundaria conectada a una instancia de EC2 está asociada al grupo de seguridad?

Como resultado, cuando se detecta un cambio en la configuración de un recurso, AWS Config no solo se crea un CI para ese recurso, sino que también se genera CIs para cualquier recurso relacionado, incluidos los que tienen relaciones indirectas. Por ejemplo, cuando AWS Config detecta cambios en una instancia de Amazon EC2, crea un CI para la instancia y un CI para el grupo de seguridad asociado a la instancia.

¿Qué relaciones indirectas AWS Config admite?

Se admiten las siguientes relaciones indirectas de recursos AWS Config.

Tipo de recurso	está relacionado indirectamente con el tipo de recurso		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface` , `AWS::EC2::Subnet` , `AWS::EC2::VPNGateway` , `AWS::EC2::VPC`		
`AWS::EC2::EIP`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface`		
`AWS::EC2::Instance`	`AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::VPC`		
`AWS::EC2::NetworkInterface`	`AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::VPC`		

Tipo de recurso	está relacionado indirectamente con el tipo de recurso		
`AWS::EC2::NetworkACL`	`AWS::EC2::Subnet` , `AWS::EC2::VPC`		
`AWS::EC2::VPNConnection`	`AWS::EC2::VPNGateway` , `AWS::EC2::CustomerGateway`		
`AWS::EC2::InternetGateway`	`AWS::EC2::VPC`		
`AWS::EC2::SecurityGroup`	`AWS::EC2::VPC`		
`AWS::EC2::Subnet`	`AWS::EC2::VPC`		
`AWS::EC2::VPNGateway`	`AWS::EC2::VPC`		

¿Qué escenarios utilizan relación indirecta?

A continuación se muestran los AWS servicios y la función del servicio que utilizan una relación indirecta.

AWS característica	Escenario
AWS Config regla gestionada	La regla ec2- security-group-attached-to - eni comprueba si los grupos de seguridad

AWS característica	Escenario
	no predeterminados están conectados a las interfaces de red elásticas (ENI). Sin una relación indirecta, tendría que crear una regla personalizada para comprobar si los grupos de seguridad no predeterminados están conectados a un ENI.
AWS Firewall Manager	La política Grupo de seguridad de auditoría de uso utiliza una relación indirecta para saber cuándo se utilizó un grupo de seguridad por última vez. Sin una relación indirecta, tendría que crear y asociar un grupo de seguridad a los nuevos recursos al mismo tiempo para evitar activar la regla con ellos. AWS Firewall Manager

AWS característica	Escenario

Recursos predeterminados	• Recursos predeterminados cuando se crea una VPC no predeterminada:
	  • Grupo de seguridad predeterminado, ACL de red predeterminada y tabla de enrutamiento predeterminada.
	• Recursos predeterminados cuando se crea una VPC predeterminada:
	  • Todo lo que se crea con una VPC predeterminada, una puerta de enlace de Internet y una subred predeterminada en cada zona de disponibilidad a la que tenga acceso.
	• Creación de una VPC predeterminada cuando una cuenta llama a EC2 por primera vez.
	  • Se crea una subred predeterminada para cuentas en una zona de disponibilidad recién lanzada.
	
	Sin una relación indirecta, tendría que esperar hasta 12 horas para que la línea de base automática registrara cambios en los recursos predeterminados.

¿Cómo se crean los elementos de configuración según la relación directa e indirecta?

En el caso de una relación directa entre los recursos (A→B), cualquier cambio de configuración en el recurso B también iniciará un elemento de configuración (CI) para el recurso A. Del mismo modo, para una relación indirecta (B→A), cuando se produce un cambio de configuración en el recurso A, se genera un nuevo CI para el recurso B. Por ejemplo, la instancia de Amazon EC2 con el grupo de seguridad tienen una relación directa, por lo que cualquier cambio de configuración en un grupo de

seguridad generará un CI para el grupo de seguridad y un CI para la instancia de EC2. Del mismo modo, el grupo de seguridad con la instancia de Amazon EC2 tienen una relación indirecta, por lo que cualquier cambio de configuración en una instancia de EC2 generaría un CI para la instancia de Amazon EC2 y un CI para el grupo de seguridad.

¿Cuáles son los elementos de configuración que se generan por las relaciones indirectas?

A continuación, se muestran los elementos de configuración adicionales (CIs) generados debido a las relaciones indirectas entre los recursos.

Cambios de configuración de los siguientes tipos de recurso	se generará CIs para los siguientes tipos de recursos		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface` , `AWS::EC2::Subnet` , `AWS::EC2::VPNGateway` y `AWS::EC2::VPC`		
`AWS::EC2::EIP`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface`		
`AWS::EC2::Instance`	`AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::VPC`		

Cambios de configuración de los siguientes tipos de recurso	se generará CIs para los siguientes tipos de recursos		
`AWS::EC2::NetworkInterface`	`AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::VPC`		
`AWS::EC2::NetworkACL`	`AWS::EC2::Subnet` , `AWS::EC2::VPC`		
`AWS::EC2::VPNConnection`	`AWS::EC2::VPNGateway` , `AWS::EC2::CustomerGateway`		
`AWS::EC2::InternetGateway`	`AWS::EC2::VPC`		
`AWS::EC2::SecurityGroup`	`AWS::EC2::VPC`		
`AWS::EC2::Subnet`	`AWS::EC2::VPC`		
`AWS::EC2::VPNGateway`	`AWS::EC2::VPC`		

¿Cómo deshabilito la relación indirecta?

Siga estos pasos para deshabilitar la relación indirecta:

1. Abre un AWS Support caso desde tu cuenta o desde la cuenta de administración para varias cuentas.
2. Seleccione Técnico como tipo de soporte.
3. En Servicios, seleccione AWS Config.
4. En Categoría, selecciona Otros.
5. Seleccione el nivel de gravedad adecuado.
6. Escriba Deshabilitar relación indirecta en la línea de asunto.
7. En la descripción:
   - Confirme que ha leído estas preguntas frecuentes y que quiere continuar.
   - Enumere las regiones en las que desee deshabilitar la relación indirecta.
   - Si lo envía desde una cuenta de administración, incluya la cuenta IDs y sus regiones asociadas.
   - En el caso de varias cuentas, puedes adjuntar un archivo CSV con la cuenta IDs y las regiones.

Un AWS Support ingeniero le proporcionará los próximos pasos y las actualizaciones de estado. Le recomendamos que mantenga una lista de AWS cuentas y regiones en las que la relación indirecta esté deshabilitada. En el caso de cuentas nuevas, envía un nuevo AWS Support caso para deshabilitar la relación indirecta.

¿Cómo puedo obtener los datos de configuración vinculados con las relaciones indirectas?

Puede ejecutar consultas de lenguaje de consulta estructurado (SQL) en las consultas AWS Config avanzadas para recuperar los datos de configuración relacionados con las relaciones indirectas de los recursos. Por ejemplo, si desea recuperar la lista de instancias de Amazon EC2 relacionadas con un grupo de seguridad, utilice la siguiente consulta:

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

Ejemplos de código para AWS Config usar AWS SDKs

Los siguientes ejemplos de código muestran cómo usarlo AWS Config con un kit de desarrollo de AWS software (SDK).

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Config Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- Ejemplos básicos de AWS Config uso AWS SDKs
  - Acciones para AWS Config usar AWS SDKs
    - Úselo DeleteConfigRule con un AWS SDK o CLI
    - Utilizar DescribeComplianceByConfigRule con una CLI
    - Utilizar DescribeComplianceByResource con una CLI
    - Utilizar DescribeConfigRuleEvaluationStatus con una CLI
    - Úselo DescribeConfigRules con un AWS SDK o CLI
    - Utilizar DescribeConfigurationRecorderStatus con una CLI
    - Utilizar DescribeConfigurationRecorders con una CLI
    - Utilizar DescribeDeliveryChannels con una CLI
    - Utilizar GetComplianceDetailsByConfigRule con una CLI
    - Utilizar GetComplianceDetailsByResource con una CLI
    - Utilizar GetComplianceSummaryByConfigRule con una CLI
    - Utilizar GetComplianceSummaryByResourceType con una CLI
    - Úselo PutConfigRule con un AWS SDK o CLI
    - Utilizar PutDeliveryChannel con una CLI

Ejemplos básicos de AWS Config uso AWS SDKs

Los siguientes ejemplos de código muestran cómo utilizar los conceptos básicos de AWS Config with AWS SDKs.

Ejemplos

- Acciones para AWS Config usar AWS SDKs
  - Úselo DeleteConfigRule con un AWS SDK o CLI
  - Utilizar DescribeComplianceByConfigRule con una CLI
  - Utilizar DescribeComplianceByResource con una CLI
  - Utilizar DescribeConfigRuleEvaluationStatus con una CLI
  - Úselo DescribeConfigRules con un AWS SDK o CLI
  - Utilizar DescribeConfigurationRecorderStatus con una CLI
  - Utilizar DescribeConfigurationRecorders con una CLI
  - Utilizar DescribeDeliveryChannels con una CLI
  - Utilizar GetComplianceDetailsByConfigRule con una CLI
  - Utilizar GetComplianceDetailsByResource con una CLI
  - Utilizar GetComplianceSummaryByConfigRule con una CLI
  - Utilizar GetComplianceSummaryByResourceType con una CLI
  - Úselo PutConfigRule con un AWS SDK o CLI
  - Utilizar PutDeliveryChannel con una CLI

Acciones para AWS Config usar AWS SDKs

Los siguientes ejemplos de código muestran cómo realizar AWS Config acciones individuales con AWS SDKs. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para ver una lista completa, consulte la Referencia de la API de AWS Config.

Ejemplos

- Úselo DeleteConfigRule con un AWS SDK o CLI
- Utilizar DescribeComplianceByConfigRule con una CLI

- Utilizar DescribeComplianceByResource con una CLI
- Utilizar DescribeConfigRuleEvaluationStatus con una CLI
- Úselo DescribeConfigRules con un AWS SDK o CLI
- Utilizar DescribeConfigurationRecorderStatus con una CLI
- Utilizar DescribeConfigurationRecorders con una CLI
- Utilizar DescribeDeliveryChannels con una CLI
- Utilizar GetComplianceDetailsByConfigRule con una CLI
- Utilizar GetComplianceDetailsByResource con una CLI
- Utilizar GetComplianceSummaryByConfigRule con una CLI
- Utilizar GetComplianceSummaryByResourceType con una CLI
- Úselo PutConfigRule con un AWS SDK o CLI
- Utilizar PutDeliveryChannel con una CLI

Úselo **`DeleteConfigRule`** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar `DeleteConfigRule`.

CLI

AWS CLI

Para eliminar una regla de AWS Config

El siguiente comando elimina una regla de AWS Config denominada`MyConfigRule`:

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Para obtener más información sobre la API, consulte DeleteConfigRulela Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Para obtener más información sobre la API, consulta DeleteConfigRulela AWS Referencia de API de SDK for Python (Boto3).

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
lo_cfs->deleteconfigrule( iv_rule_name ).
MESSAGE 'Deleted AWS Config rule.' TYPE 'I'.
```

- Para obtener más información sobre la API, consulte DeleteConfigRulela referencia sobre la API ABAP del AWS SDK para SAP.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Config Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`DescribeComplianceByConfigRule`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeComplianceByConfigRule`.

CLI

AWS CLI

Para obtener información sobre el cumplimiento de tus reglas de AWS Config

El siguiente comando devuelve la información de conformidad de cada regla de AWS Config que uno o más AWS recursos infrinjan:

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

En el resultado, el valor de cada atributo de `CappedCount` indica cuántos recursos no cumplen con la regla relacionada. Por ejemplo, el siguiente resultado indica que tres recursos no cumplen con la regla denominada `InstanceTypesAreT2micro`.

Salida:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeComplianceByConfigRulela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Este ejemplo recupera los detalles de conformidad de la regla ebs-optimized-instance, para los que no hay resultados de evaluación actuales, por lo que devuelve INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Salida:

```
ComplianceContributorCount ComplianceType
------------------------- --------------
                           INSUFFICIENT_DATA
```

Ejemplo 2: Este ejemplo devuelve el número de recursos no conformes para la regla ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Salida:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Para obtener más información sobre la API, consulte Cmdlet Reference (V4 DescribeComplianceByConfigRule).Herramientas de AWS para PowerShell

Herramientas para la versión 5 PowerShell

Ejemplo 1: Este ejemplo recupera los detalles de conformidad de la regla ebs-optimized-instance, para los que no hay resultados de evaluación actuales, por lo que devuelve INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Salida:

```
ComplianceContributorCount ComplianceType
------------------------- --------------
                           INSUFFICIENT_DATA
```

Ejemplo 2: Este ejemplo devuelve el número de recursos no conformes para la regla ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Salida:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Para obtener más información sobre la API, consulte Cmdlet Reference (V5 DescribeComplianceByConfigRule).Herramientas de AWS para PowerShell

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`DescribeComplianceByResource`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeComplianceByResource`.

CLI

AWS CLI

Para obtener información sobre el cumplimiento de sus AWS recursos

El siguiente comando devuelve la información de conformidad de cada instancia EC2 grabada por AWS Config y que infringe una o más reglas:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

En el resultado, el valor de cada atributo de `CappedCount` indica cuántas reglas infringe el recurso. Por ejemplo, el siguiente resultado indica que la instancia `i-1a2b3c4d` infringe dos reglas.

Salida:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
```

```
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeComplianceByResourcela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se revisa el tipo de recurso **`AWS::SSM::ManagedInstanceInventory`** para el tipo de cumplimiento COMPLIANT.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Salida:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
```

```
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Para obtener más información sobre la API, consulte DescribeComplianceByResource Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se revisa el tipo de recurso **`AWS::SSM::ManagedInstanceInventory`** para el tipo de cumplimiento COMPLIANT.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Salida:

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Para obtener más información sobre la API, consulte DescribeComplianceByResourcela referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`DescribeConfigRuleEvaluationStatus`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeConfigRuleEvaluationStatus`.

CLI

AWS CLI

Para obtener información de estado de una regla de AWS Config

El siguiente comando devuelve la información de estado de una regla de AWS Config denominada`MyConfigRule`:

```
aws configservice describe-config-rule-evaluation-status --config-rule-
names MyConfigRule
```

Salida:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeConfigRuleEvaluationStatusla Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Este ejemplo devuelve la información de estado de las reglas de configuración correspondientes.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Salida:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
```

```
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- Para obtener más información sobre la API, consulte DescribeConfigRuleEvaluationStatus Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Este ejemplo devuelve la información de estado de las reglas de configuración correspondientes.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Salida:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
```

```
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- Para obtener más información sobre la API, consulte DescribeConfigRuleEvaluationStatusla referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeConfigRules`** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeConfigRules`.

CLI

AWS CLI

Para obtener detalles de una regla de AWS Config

El siguiente comando devuelve los detalles de una regla de AWS Config denominada`InstanceTypesAreT2micro`:

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Salida:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeConfigRuleslla Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se enumeran las reglas de configuración de la cuenta, con las propiedades seleccionadas.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Salida:

```
ConfigRuleName                                    ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                    ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                             config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                               config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required        config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Para obtener más información sobre la API, consulte DescribeConfigRules Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se enumeran las reglas de configuración de la cuenta, con las propiedades seleccionadas.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Salida:

```
ConfigRuleName                                    ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                    ------------
 -------------
 ---------------
```

```
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Para obtener más información sobre la API, consulte DescribeConfigRuleslla referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
```

```
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Para obtener más información sobre la API, consulta DescribeConfigRuleslа AWS Referencia de API de SDK for Python (Boto3).

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    DATA(lo_result) = lo_cfs->describeconfigrules(
      it_configrulenames = VALUE /aws1/
cl_cfsconfigrulenames_w=>tt_configrulenames(
        ( NEW /aws1/cl_cfsconfigrulenames_w( iv_rule_name ) )
      )
    ).
    ot_cfg_rules = lo_result->get_configrules( ).
    MESSAGE 'Retrieved AWS Config rule data.' TYPE 'I'.
```

- Para obtener más información sobre la API, consulte DescribeConfigRuleslа referencia sobre la API ABAP del AWS SDK para SAP.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Config Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`DescribeConfigurationRecorderStatus`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeConfigurationRecorderStatus`.

CLI

AWS CLI

Información sobre el estado en el registro de configuración

El siguiente comando devuelve el estado del registro de configuración predeterminado:

```
aws configservice describe-configuration-recorder-status
```

Salida:

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeConfigurationRecorderStatusla Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Este ejemplo devuelve el estado de los registros de configuración.

```
Get-CFGConfigurationRecorderStatus
```

Salida:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- Para obtener más información sobre la API, consulte DescribeConfigurationRecorderStatus Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Este ejemplo devuelve el estado de los registros de configuración.

```
Get-CFGConfigurationRecorderStatus
```

Salida:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- Para obtener más información sobre la API, consulte DescribeConfigurationRecorderStatusla referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`DescribeConfigurationRecorders`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeConfigurationRecorders`.

CLI

AWS CLI

Información sobre el registro de configuración

El comando siguiente devuelve información sobre el registro de configuración predeterminado:

```
aws configservice describe-configuration-recorders
```

Salida:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeConfigurationRecordersla Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Este ejemplo devuelve información sobre los registros de configuración.

```
Get-CFGConfigurationRecorder | Format-List
```

Salida:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- Para obtener más información sobre la API, consulte DescribeConfigurationRecorders Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Este ejemplo devuelve información sobre los registros de configuración.

```
Get-CFGConfigurationRecorder | Format-List
```

Salida:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- Para obtener más información sobre la API, consulte DescribeConfigurationRecordersla referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`DescribeDeliveryChannels`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeDeliveryChannels`.

CLI

AWS CLI

Información sobre el canal de entrega

El comando siguiente devuelve información detallada sobre el canal de entrega:

```
aws configservice describe-delivery-channels
```

Salida:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte DescribeDeliveryChannelsla Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se recupera el canal de entrega de la región y se muestran los detalles.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Salida:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Para obtener más información sobre la API, consulte DescribeDeliveryChannels Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se recupera el canal de entrega de la región y se muestran los detalles.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Salida:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Para obtener más información sobre la API, consulte DescribeDeliveryChannelsla referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`GetComplianceDetailsByConfigRule`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Para obtener los resultados de la evaluación de una regla de AWS Config

El siguiente comando devuelve los resultados de la evaluación de todos los recursos que no cumplen con una regla de AWS Config denominada`InstanceTypesAreT2micro`:

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Salida:

```
{
    "EvaluationResults": [
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Para obtener más información sobre la API, consulta GetComplianceDetailsByConfigRulela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo se obtienen los resultados de la evaluación de la regla access-keys-rotated y se devuelve el resultado agrupado por tipo de conformidad

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Salida:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Ejemplo 2: En este ejemplo se consultan los detalles de conformidad de la regla access-keys-rotated para los recursos de COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Salida:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Para obtener más información sobre la API, consulte GetComplianceDetailsByConfigRule Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo se obtienen los resultados de la evaluación de la regla access-keys-rotated y se devuelve el resultado agrupado por tipo de conformidad

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Salida:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Ejemplo 2: En este ejemplo se consultan los detalles de conformidad de la regla access-keys-rotated para los recursos de COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Salida:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Para obtener más información sobre la API, consulte GetComplianceDetailsByConfigRule Herramientas de AWS para PowerShellCmdlet Reference (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`GetComplianceDetailsByResource`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetComplianceDetailsByResource`.

CLI

AWS CLI

Para obtener los resultados de la evaluación de un AWS recurso

El siguiente comando devuelve los resultados de la evaluación para cada regla infringida por la instancia de EC2 `i-1a2b3c4d`:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Salida:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
```

```
}
```

- Para obtener más información sobre la API, consulte GetComplianceDetailsByResourcela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Este ejemplo devuelve los resultados de la evaluación de un recurso determinado.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Salida:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Para obtener más información sobre la API, consulte GetComplianceDetailsByResource Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Este ejemplo devuelve los resultados de la evaluación de un recurso determinado.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Salida:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
```

```
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Para obtener más información sobre la API, consulte GetComplianceDetailsByResourcela referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`GetComplianceSummaryByConfigRule`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Para obtener el resumen de conformidad de tus reglas de AWS Config

El comando siguiente devuelve el número de reglas conformes y el de las reglas no conformes:

```
aws configservice get-compliance-summary-by-config-rule
```

En el resultado, el valor de cada atributo `CappedCount` indica el número de reglas conformes o no conformes.

Salida:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
```

```
        }
    }
}
```

- Para obtener más información sobre la API, consulta GetComplianceSummaryByConfigRulela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Este ejemplo devuelve el número de reglas de Config que no son conformes.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Salida:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByConfigRule Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Este ejemplo devuelve el número de reglas de Config que no son conformes.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Salida:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByConfigRulela referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`GetComplianceSummaryByResourceType`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Resumen de conformidad para todos los tipos de recursos

El siguiente comando devuelve el número de AWS recursos que no son compatibles y el número que sí lo son:

```
aws configservice get-compliance-summary-by-resource-type
```

En el resultado, el valor de cada atributo `CappedCount` indica el número de recursos conformes y el de no conformes.

Salida:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Obtención del resumen de conformidad de un tipo de recurso específico

El comando siguiente devuelve el número de instancias de EC2 no conformes y el número de las conformes:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

En el resultado, el valor de cada atributo `CappedCount` indica el número de recursos conformes y el de no conformes.

Salida:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByResourceTypela Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se devuelve el número de recursos conformes y no conformes, y se convierte el resultado en json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByResourceType Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se devuelve el número de recursos conformes y no conformes, y se convierte el resultado en json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Para obtener más información sobre la API, consulte GetComplianceSummaryByResourceTypela referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`PutConfigRule`** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran cómo utilizar `PutConfigRule`.

CLI

AWS CLI

Para añadir una regla de Config AWS gestionada

El siguiente comando proporciona código JSON para añadir una regla de Config AWS gestionada:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` es un archivo JSON que contiene la configuración de la regla:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Para el `ComplianceResourceTypes` atributo, este código JSON limita el alcance a los recursos de este `AWS::EC2::Instance` tipo, por lo que AWS Config evaluará solo las

instancias de EC2 según la regla. Puesto que la regla es una regla administrada, el atributo `Owner` se establece en `AWS` y el atributo `SourceIdentifier` en el identificador de la regla, `REQUIRED_TAGS`. Para el atributo `InputParameters`, se especifican las claves de etiqueta que requiere la regla, `CostCenter` y `Owner`.

Si el comando se ejecuta correctamente, AWS Config no devuelve ningún resultado. Para verificar la configuración de la regla, ejecute el describe-config-rules comando y especifique el nombre de la regla.

Adición de una regla de configuración administrada por el cliente

En el siguiente comando se proporciona un código JSON para añadir una regla de configuración administrada por el cliente:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` es un archivo JSON que contiene la configuración de la regla:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Para el `ComplianceResourceTypes` atributo, este código JSON limita el alcance a los recursos de este `AWS::EC2::Instance` tipo, por lo que AWS Config evaluará solo las instancias de EC2 según la regla. Como esta regla es una regla administrada por el cliente, el `Owner` atributo se establece en y el `SourceIdentifier` atributo se establece en el ARN de la función Lambda AWS . `CUSTOM_LAMBDA` El objeto `SourceDetails` es obligatorio. Los parámetros que se especifican para el `InputParameters` atributo se pasan a la función AWS Lambda cuando AWS Config la invoca para evaluar los recursos en función de la regla.

Si el comando se ejecuta correctamente, AWS Config no devuelve ningún resultado. Para verificar la configuración de la regla, ejecute el describe-config-rules comando y especifique el nombre de la regla.

- Para obtener más información sobre la API, consulte PutConfigRulela Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
```

```
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Para obtener más información sobre la API, consulta PutConfigRulela AWS Referencia de API de SDK for Python (Boto3).

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    " Create a config rule for S3 bucket public read prohibition
    lo_cfs->putconfigrule(
      io_configrule = NEW /aws1/cl_cfsconfigrule(
        iv_configrulename = iv_rule_name
        iv_description = |S3 Public Read Prohibited Bucket Rule|
        io_scope = NEW /aws1/cl_cfsscope(
          it_complianceresourcetypes = VALUE /aws1/
cl_cfscplncresrctypes_w=>tt_complianceresourcetypes(
            ( NEW /aws1/cl_cfscplncresrctypes_w( |AWS::S3::Bucket| ) )
          )
        )
        io_source = NEW /aws1/cl_cfssource(
          iv_owner = |AWS|
          iv_sourceidentifier = |S3_BUCKET_PUBLIC_READ_PROHIBITED|
        )
        iv_inputparameters = '{}'
        iv_configrulestate = |ACTIVE|
      )
    ).
    MESSAGE 'Created AWS Config rule.' TYPE 'I'.
```

- Para obtener más información sobre la API, consulte PutConfigRulela referencia sobre la API ABAP del AWS SDK para SAP.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Config Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`PutDeliveryChannel`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `PutDeliveryChannel`.

CLI

AWS CLI

Creación de un canal de entrega

El siguiente comando proporciona la configuración del canal de entrega en forma de código JSON:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

El archivo `deliveryChannel.json` especifica los atributos del canal de entrega:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Este ejemplo establece los siguientes atributos:

`name`: El nombre del canal de entrega. De forma predeterminada, AWS Config asigna el nombre `default` a un nuevo canal de entrega. No puede actualizar el nombre del canal de entrega con el comando. `put-delivery-channel` Si desea saber cuáles son los pasos para cambiar el nombre, consulte Renaming the Delivery Channel. `s3BucketName`: - El nombre del bucket de Amazon S3 al que AWS Config entrega las instantáneas de configuración y los archivos del historial de configuración. Si especifica un bucket que pertenece a otra AWS cuenta, ese bucket debe tener políticas que concedan permisos de acceso a Config. AWS Para obtener más información, consulte Permisos para el bucket de Amazon S3.

`snsTopicARN`- El nombre del recurso de Amazon (ARN) del tema de Amazon SNS al que AWS Config envía notificaciones sobre los cambios de configuración. Si elige un tema de otra cuenta, el tema debe tener políticas que concedan permisos de acceso a Config. AWS Para obtener más información, consulte Permissions for the Amazon SNS Topic.

`configSnapshotDeliveryProperties`- Contiene el `deliveryFrequency` atributo, que establece la frecuencia con la que AWS Config entrega instantáneas de la configuración y la frecuencia con la que invoca las evaluaciones de las reglas de Config periódicas.

Si el comando se ejecuta correctamente, AWS Config no devuelve ningún resultado. Para verificar la configuración de su canal de entrega, ejecute el describe-delivery-channels comando.

- Para obtener más información sobre la API, consulte PutDeliveryChannella Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: En este ejemplo, se cambia la propiedad deliveryFrequency de un canal de entrega existente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- Para obtener más información sobre la API, consulte PutDeliveryChannel Herramientas de AWS para PowerShellCmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: En este ejemplo, se cambia la propiedad deliveryFrequency de un canal de entrega existente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- Para obtener más información sobre la API, consulte PutDeliveryChannella referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Config Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Historial de documentos

En la siguiente tabla se describen los cambios importantes en la documentación de AWS Config. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

- Versión de la API: 2014-11-12
- Última actualización de la documentación: 27 de enero de 2026

Cambio	Descripción	Fecha
Actualizaciones de seguridad de IAM	Las `AWS_ConfigRole` políticas `AWSConfigServiceRolePolicy` y las políticas se han actualizado con permisos exhaustivos para el registro de la configuración de los AWS recursos en más de 100 AWS servicios. Para más información, consulte Políticas administradas de AWS para AWS Config.	27 de enero de 2026
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • cloudformation-stack-service-role-comprobar • cloudfront-distribution-key-group-habilitado • ecs-capacity-provider-termination-comprobar	9 de enero de 2026

	• ecs-task-definition-linux-user-non-root • ecs-task-definition-windows-user-non-admin	
AWS Config admite los nuevos permisos necesarios para las tablas S3	Con esta versión, AWS Config se agregaron los nuevos permisos necesarios para registrar los tipos de recursos de las tablas S3. Para obtener más información, consulte Tipos de recursos compatibles.	9 de enero de 2026
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • aurora-global-database-encryption-en reposo • cloudformation-termination-protection-check • cognito-userpool-cust-auth-threat-full-check • cognito-user-pool-deletion-habilitada para la protección • cognito-user-pool-mfa-habilitado • ebs-snapshot-block-public-acceso • ecs-task-definition-efs-habilitado para el cifrado • ses-sending-tls-required	8 de diciembre de 2025

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • aurora-global-database-encryption-en reposo • cloudformation-termination-protection-check • cognito-userpool-cust-auth-threat-full-check • cognito-user-pool-deletion-habilitada para la protección • cognito-user-pool-mfa-habilitado • ebs-snapshot-block-public-acceso • ecs-task-definition-efs-habilitado para el cifrado • ses-sending-tls-required	8 de diciembre de 2025
???	El ejemplo de la política de bucket multicuenta de S3 ya no incluye al director `config.amazonaws.com` de servicio. Para obtener más información, consulte required-permissions-cross-account.	3 de diciembre de 2025

Actualizaciones de seguridad de IAM	Las `AWS_ConfigRole` políticas `AWSConfigServiceRolePolicy` y ahora otorgan permisos adicionales para Amazon Lightsail y Amazon Simple Storage Service (Amazon S3). Para más información, consulte Políticas administradas de AWS para AWS Config.	20 de noviembre de 2025
Actualización de seguridad de IAM	AWS Config ha actualizado la política gestionada `AWSConfigServiceRolePolicy` con una documentación mejorada sobre permisos exhaustivos para el registro de la configuración de AWS recursos en más de 100 AWS servicios. Para obtener más información, consulte AWS Config las actualizaciones de las políticas AWS gestionadas.	11 de noviembre de 2025
Actualización de seguridad de IAM	AWS Config ha actualizado la política gestionada `AWS_ConfigRole` con permisos integrales para el registro de la configuración de los AWS recursos en varios servicios. Para más información, consulte Políticas administradas de AWS para AWS Config.	10 de noviembre de 2025

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • amplify-app-no-environment-variables • amplify-branch-description • api-gwv2- -habilitada para métricas stage-default-route-detailed • apigateway-stage-description • apigatewayv2-stage-description • appconfig-deployment-strategy-tagged • aps-rule-groups-namespace-etiquetado • auditmanager-assessment-tagged • batch-managed-spot-compute-environment-max-bid • cognito-identity-pool-unauthenticated-inicios de sesión • customerprofiles-domain-tagged • devicefarm-project-tagged • devicefarm-test-grid-project-etiquetado • ec2- network-insights-analysis-tagged • eks-fargate-profile-tagged	27 de octubre de 2025

- glue-ml-transform-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-video-stream-minimum-retención de datos
- lambda-function-description
- lightsail-bucket-allow-public-anula - deshabilitado
- ruta 53- - etiquetada resolver-firewall-domain-list
- ruta 53- -asociacion-etiquetada resolver-firewall-rule-group
- ruta 53- resolver-firewall-rule-group - etiquetada
- ruta 53 - resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-habilitada para registros
- rum-app-monitor-tagged

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los nuevos tipos de AWS Config recursos y Amazon API Gateway. AWS CloudTrail Para obtener más información, consulte Tipos de recursos compatibles.	10 de octubre de 2025
AWS Config es compatible con el nuevo paquete de conformidad	Con esta versión, AWS Config es compatible con el siguiente paquete de conformidad: Cyber Resilience Best Practices for Amazon S3, Amazon EBS y Amazon DynamoDB	3 de octubre de 2025

Actualizaciones de seguridad de IAM	Las `AWS_ConfigRole` políticas `AWSConfig ServiceRolePolicy` y ahora otorgan permisos adicionales para AWS Amplify AWS AppSync, Amazon Bedrock,, AWS CloudTrai l, CloudFormation AWS CodeArtifact, Amazon Connect AWS CodePipeline, Amazon EC2 AWS Deadline Cloud,, Amazon IVS AWS Entity Resolution AWS IoT SiteWise, Amazon, Amazon Quick AWS Lambda EventBridge, Amazon Redshift, Amazon Redshift Serverless AWS Identity and Access Management Roles Anywhere, Amazon, Amazon Security Lake AWS Service Catalog, SageMaker AWS Secrets Manager AWS Shield Amazon EC2 Systems Manager y. AWS WAFV2 Para más información, consulte Políticas administradas de AWS para AWS Config.	1 de octubre de 2025

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config admite las siguientes reglas administradas: • cognito-user-pool-password-verificación de políticas • dms-replication-instance-multi-az-habilitado • ec2- -encriptado launch-templates-ebs-volume • rds-mysql-cluster-copy-tags-to-snapshot-check • rds-pgsql-cluster-copy-tags-to-snapshot-check	1 de octubre de 2025
AWS Config admite nuevos tipos de recursos en la región de Asia Pacífico (Taipéi)	Con esta versión, AWS Config ahora es compatible con los siguientes tipos de AWS WAFV2 recursos en la región de Asia Pacífico (Taipéi): • AWS:WAFv2:: IPSet • AWS::WAFv2::ManagedRuleSet • AWS::WAFv2::RegexPatternSet • AWS::WAFv2::RuleGroup • AWS::WAFv2::WebACL Para obtener información, consulte Cobertura de recursos según la disponibilidad por región.	23 de septiembre de 2025

AWS Config actualiza los paquetes de conformidad	Con esta versión, AWS Config se han actualizado los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para ACSC Essential 8 • Prácticas operativas recomendadas para ACSC ISM: parte 2	9 de septiembre de 2025
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los tipos de recursos nuevos AWS CodeArtifact AWS Config AWS Glue, AWS Network Manager,, y de AWS Identity and Access Management recursos. Para obtener más información, consulte Tipos de recursos compatibles.	3 de septiembre de 2025

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los nuevos tipos de AWS Backup recursos de Amazon OpenSearch Service, Amazon EC2, Amazon Managed Streaming for Apache Kafka for Apache Kafka, Amazon Redshift, Route 53 Administrador de incidentes de AWS Systems Manager Profiles AWS Transfer Family y Amazon. CloudFront Para obtener más información, consulte Tipos de recursos compatibles.	15 de agosto de 2025
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • cloudfront-origin-lambda-url-activado para oac • sqs-queue-policy-full-control de acceso • sqs-queue-dlq-check	14 de agosto de 2025

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • alb-tagged • api-gw-rest-api-etiquetado • api-gw-stage-tagged • appsync-graphql-api-xray-habilitado • cloudwatch-metric-stream-tagged • codebuild-report-group-tagged • datasync-location-object-storage-usando-https • ec2- vpn-connection-tagged • ecs-capacity-provider-tagged • efs-file-system-tagged • eks-addon-tagged • elb-internal-scheme-check • elb-tagged • glb-tagged • iot-job-template-tagged • iotdevicedefender-custom-metric-tagged • kms-key-tagged • msk-cluster-tagged • nlb-tagged • rds-event-subscription-tagged • rds-option-group-tagged	13 de agosto de 2025

- ruta 53- health-check-tagge d
- ruta 53- hosted-zone-tagged
- service-catalog-portfolio-t agged
- stepfunctions-state-machine -tagged
- workspaces-connection- alias-tagged
- workspaces-workspace- tagged

Actualizaciones de seguridad de IAM	La `AWS_ConfigRole` política ahora otorga permisos adicionales para Amazon Bedrock AWS ARC - Zonal Shift,,,, AWS CloudTrail, AWS CodeArtifact AWS Deadline Cloud AWS Database Migration Service AWS Glue AWS Identity and Access Management, Amazon Managed Streaming for Apache Kafka Kafka AWS Lake Formation, CloudWatch Amazon Logs AWS Elemental MediaLive, AWS Elemental MediaPack age, Amazon Relational Database Service, Amazon Simple Storage Service AWS Secrets Manager, Amazon Security Lake AWS Service Catalog, Amazon Simple Email Service y. AWS X-Ray Para más información, consulte Políticas administradas de AWS para AWS Config.	28 de julio de 2025

Actualizaciones de seguridad de IAM	La `AWSConfigServiceRolePolicy` política ahora concede permisos adicionales para Amazon Bedrock AWS ARC - Zonal Shift,,,, AWS CloudTrail, AWS CodeArtifact AWS Deadline Cloud AWS Database Migration Service AWS Glue AWS Identity and Access Management, Amazon Managed Streaming for Apache Kafka Kafka AWS Lake Formation, CloudWatch Amazon Logs AWS Elemental MediaLive, AWS Elemental MediaPackage, Amazon Relational Database Service, Amazon Simple Storage Service AWS Secrets Manager, Amazon Security Lake AWS Service Catalog, Amazon Simple Email AWS X-Ray Service y Amazon API Gateway. Para más información, consulte Políticas administradas de AWS para AWS Config.	28 de julio de 2025

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos AWS Backup CloudFront tipos AWS Entity Resolutio n de recursos de Amazon Relational Database Service y Amazon S3. Administración de facturación y costos de AWS CloudFormation AWS IoT AWS Private Certificate Authority Para obtener más información, consulte Tipos de recursos compatibles.	15 de julio de 2025

Actualizaciones de seguridad de IAM	La `AWS_ConfigRole` política y la `AWSConfig ServiceRolePolicy` política ahora otorgan permisos adicionales para AWS Backup gateway Amazon Bedrock, Amazon, AWS CloudFormation, CloudFront,, AWS Entity Resolution, AWS IoT Core Device Advisor AWS Lambda AWS Network Manager, Amazon Redshift AWS Private Certificate Authority, Amazon S3 Tables,. Administración de facturación y costos de AWS Quick Setup de AWS Systems Manager Para más información, consulte Políticas administradas de AWS para AWS Config.	18 de junio de 2025
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon Bedrock. Para obtener más información, consulte Tipos de recursos compatibles.	17 de junio de 2025

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • cloudfront-ssl-policy-check • cognito-identity-pool-unauth-comprobación de acceso • ec2- -habilitado enis-source-destination-check • elbv2- listener-encryption-in-transit • lambda-function-xray-enabled • msk-cluster-public-access-deshabilitado • msk-connect-connector-logging-habilitado • msk-unrestricted-access-check • aurora-mysql-cluster-audit-registro • redshift-cluster-multi-az-habilitado • s3 -rules-check express-dir-bucket-lifecycle • ssm-automation-logging-enabled • ssm-automation-block-public-compartir	13 de junio de 2025

Actualización de seguridad de IAM	La política `AWSConfigServiceRolePolicy` y la política `AWS_ConfigRole` conceden ahora permisos adicionales para Amazon Bedrock. Para más información, consulte Políticas administradas de AWS para AWS Config.	27 de mayo de 2025
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon App Integrations, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Inspector, Amazon Macie, Amazon Route 53 Profiles, OpenSearch Amazon Serverless, Amazon Simple Storage Service (Amazon S3) y Amazon AI. AWS Security Hub CSPM SageMaker Para obtener más información, consulte Tipos de recursos admitidos.	30 de abril de 2025
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config admite la siguiente regla administrada: redshift-serverless-default-db-name-check	22 de abril de 2025

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con la siguiente regla gestionada: redshift-serverless-default-admin-check	17 de abril de 2025
Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Bedrock Intercambio de datos de AWS B2B,,, AWS Database Migration Service (AWS DMS) AWS Clean Rooms AWS CodeConnections, Amazon CloudWatch Logs AWS Direct Connect, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), SageMaker Amazon AI AWS Security Hub CSPM y Contacts y. Administrador de incidentes de AWS Systems Manager Administrador de incidentes de AWS Systems Manager AWS Systems Manager Para más información, consulte Políticas administradas de AWS para AWS Config.	8 de abril de 2025

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • s3-bucket-tagged • ecr-repository-tagged • sagemaker-feature-group-tagged • sagemaker-domain-tagged • cognito-user-pool-tagged	1 de abril de 2025

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config admite las siguientes reglas administradas: • nlb-cross-zone-load-habilitado para el equilibrio • redshift-serverless-publish-logs-a cloudwatch • rds-instance-subnet-igw-comprobar • ec2- - spot-fleet-request-ct encryption-at-rest • redshift-serverless-workgroup-encrypted-en tránsito • redshift-serverless-workgroup-no-acceso público • redshift-serverless-namespace-cmk-cifrado • event-data-store-cmk-habilitado para el cifrado • ecs-task-definition-network-mode-not-host • rds-proxy-tls-encryption • nlb-logging-enabled • redshift-audit-logging-enabled • s3- lifecycle-policy-check • sagemaker-image-tagged • redshift-cluster-parameter-group-etiquetado • ec2- dhcp-options-tagged • sagemaker-app-image-config-etiquetado	22 de marzo de 2025

- mariadb-publish-logs-to-registros de cloudwatch
- docdb-cluster-encrypted-in-tránsito
- rds-sqlserver-encrypted-in-tránsito
- ec2- traffic-mirror-session-tagged
- ec2- launch-template-tagged
- ec2- traffic-mirror-target-tagged
- transfer-certificate-tagged
- batch-managed-compute-env-compute-resources-tagged
- lightsail-disk-tagged
- transfer-profile-tagged
- amplify-app-tagged
- ec2- prefix-list-tagged
- amplify-branch-tagged
- transfer-agreement-tagged
- datasync-task-tagged
- transfer-workflow-tagged
- sagemaker_notebook_instance_platform_version
- ec2- traffic-mirror-filter-tagged
- aurora-mysql-cluster-audit-registro
- ssm-document-tagged
- transfer-connector-tagged

- rds-mariadb-instance-encrypted-en tránsito
- iam-saml-provider-tagged
- ec2-fleet-tagged
- iam-server-certificate-tagged
- iam-oidc-provider-tagged
- alb-listener-tagged
- glb-listener-tagged
- ec2- -etiquetado network-insights-access-scope
- lightsail-certificate-tagged
- ec2- capacity-reservation-tagged
- ec2- -etiquetado transit-gateway-multicast-domain
- dms-endpoint-tagged
- ec2- carrier-gateway-tagged
- dms-replication-task-tagged
- ec2- client-vpn-endpoint-tagged
- lightsail-bucket-tagged
- ec2- -análisis-etiquetado network-insights-access-scope
- nlb-listener-tagged
- ec2- network-insights-path-tagged

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • docdb-cluster-encrypted-in-tránsito • mariadb-publish-logs-to-cloudwatch-logs • aurora-mysql-cluster-audit-registro • rds-mariadb-instance-encrypted-en tránsito • rds-sqlserver-encrypted-in-tránsito • sagemaker-notebook-instance-platform-versión • appstream-fleet-multi-az • apprunner-vpc-connector-multi-az • mq-broker-general-logging-habilitado • mq-active-single-instance-broker-storage-type-efs • mq-active-broker-ldap-autenticación • iottwinmaker-component-type-tagged	19 de marzo de 2025

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • fsx-openzfs-deployment-type-comprobar • fsx-ontap-deployment-type-comprobar • fsx-windows-deployment-type-comprobar • redshift-serverless-workgroup-routes-dentro del vpc	18 de marzo de 2025
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: ec2- -ami instance-launched-with-allowed	11 de marzo de 2025

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config admite las siguientes reglas administradas: • connect-instance-logging-enabled • ecr-repository-cmk-encryption-habilitado • elbv2- -check predefined-security-policy-ssl • glue-spark-job-supported-versión • guardduty-runtime-monitoring-enabled • guardduty-ecs-protection-runtime-habilitado • guardduty-ec2- protection-runtime-enabled • netfw-subnet-change-protection-habilitado • rds-sql-server-logs-a cloudwatch • sqs-queue-no-public-acceso • transfer-connector-logging-enabled	7 de marzo de 2025

Actualización de seguridad de IAM	La política `AWSConfigServiceRolePolicy` y la política `AWS_ConfigRole` conceden ahora permisos adicionales para Amazon Elastic Compute Cloud (Amazon EC2). Para más información, consulte Políticas administradas de AWS para AWS Config.	4 de marzo de 2025

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config admite las siguientes reglas administradas: • athena-workgroup-descriptio n • amplify-app-tagged • sagemaker-app-image-config-etiquetado • elasticbeanstalk-application-version-description • amplify-branch-per formance-mode-habilitado • athena-workgroup-engine-version-actualización automática • sagemaker-image-de scription • devicefarm-instance-profile-tagged • transfer-workflow-descripti on • ec2- traffic-mirror-session-tagged • appstream-fleet-in-vpc • transfer-agreement-tagged • ec2- traffic-mirror-target-description • transfer-agreement-descript ion • athena-prepared-statement-description	8 de febrero de 2025

- batch-managed-compute-env-compute-resources-tagged
- codedeploy-deployment-group-auto-habilitado para la reversión
- batch-managed-compute-environment-using-launch-template
- ec2- prefix-list-tagged
- ec2- traffic-mirror-filter-tagged
- athena-workgroup-enforce-workgroup-configuración
- transfer-certificate-tagged
- batch-compute-environment-managed
- lightsail-disk-tagged
- transfer-profile-tagged
- ec2- traffic-mirror-target-tagged
- appintegrations-event-integration-tagged
- datasync-task-tagged
- batch-compute-environment-enabled
- appconfig-configuration-profile-validators-no está vacío
- elasticbeanstalk-application-description
- codedeploy-deployment-group-outdated-instancias-actualizar

- ec2- launch-template-tagged
- fis-experiment-template-tagged
- ivs-channel-playback-authorization-habilitado
- redshift-cluster-parameter-group-etiquetado
- ec2- traffic-mirror-filter-description
- appintegrations-event-integration-description
- athena-data-catalog-description
- fis-experiment-template-log-configuración- existe
- amplify-app-description
- amplify-branch-tagged
- batch-job-queue-enabled
- elasticbeanstalk-environment-description
- amplify-app-branch-auto-habilitado para eliminar
- appconfig-hosted-configuration-version-descripción
- appconfig-freeform-profile-config-almacenamiento
- datasync-task-data-verification-habilitado
- apprunner-service-observability-enabled
- transfer-certificate-description

	• appconfig-deployment-strategy-replicate-to-ssm • transfer-workflow-tagged • transfer-connector-tagged • ec2- traffic-mirror-session-description • customerprofiles-object-type-allow-creación de perfil • sagemaker-image-tagged	
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte Tipos de recursos admitidos.	6 de febrero de 2025
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte Tipos de recursos admitidos.	29 de enero de 2025

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Comprehend AWS Clean Rooms, Amazon Elastic Compute Cloud (Amazon EC2) AWS HealthOmics, Amazon Simple Storage Service (Amazon S3) y Amazon Simple Email Service (Amazon SES). Para más información, consulte Políticas administradas de AWS para AWS Config.	16 de enero de 2025

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config admite las siguientes reglas administradas: • appmesh-mesh-deny-tcp-reenvío • sagemaker-model-isolation-enabled • evidently-project-description • alb-internal-scheme-check • evidently-segment-descripti on • appconfig-environment-description • apprunner-service-in-vpc • sagemaker-domain-in-vpc • nlb-internal-scheme-check • emr-security-configuration-encryption-descansar • apprunner-service-no-public-acceso • sagemaker-model-in-vpc • appconfig-deployment-strategy-description • evidently-launch-description • iot-authorizer-token-signing-habilitado	9 de enero de 2025

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon Elastic Compute Cloud (Amazon EC2). Para obtener más información, consulte Tipos de recursos admitidos.	9 de enero de 2025

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config admite las siguientes reglas administradas: • batch-job-queue-tagged • iottwinmaker-sync-job-tagged • codeguruprofiler-profiling-group-tagged • ivs-recording-configuration-tagged • iottwinmaker-entity-tagged • iottwinmaker-workspace-tagged • iottwinmaker-scene-tagged • acmpca-certificate-authority-tagged • appflow-flow-tagged • iotevents-detector-model-tagged • appmesh-virtual-node-logging-file-path-exists • apprunner-vpc-connector-tagged • apprunner-service-tagged • iotwireless-fuota-task-tagged • appmesh-virtual-node-backend-defaults-tls-on • codegurureviewer-repository-association-tagged • iotevents-input-tagged	8 de enero de 2025

- appmesh-virtual-gateway-logging-file-path-exists
- batch-compute-environment-tagged
- batch-scheduling-policy-tagged
- customerprofiles-object-type-tagged
- emr-security-configuration-encryption-tránsito
- iotwireless-service-profile-tagged
- ivs-playback-key-pair-etiquetado
- cassandra-keyspace-tagged
- iotevents-alarm-model-tagged
- appconfig-application-description
- appmesh-virtual-gateway-backend-defaults-tls
- ivs-channel-tagged
- iotwireless-multicast-group-tagged

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon Elastic Compute Cloud (Amazon EC2) AWS Elemental MediaConnect, Amazon Cognito y OpenSearch Amazon Service. Para obtener más información, consulte Tipos de recursos admitidos.	19 de diciembre de 2024
Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política ahora otorga permisos adicionales para. AWS Organizations Para más información, consulte Políticas administradas de AWS para AWS Config.	18 de diciembre de 2024

AWS Config admite grabadores de configuración vinculados a servicios	Con esta versión, es AWS Config compatible con los grabadores de configuración vinculados a servicios. Usted habilita un grabador de configuración vinculado a un servicio en el servicio compatible o mediante el AWS CLI, y el grabador graba los tipos de recursos necesarios para el servicio vinculado en su nombre. Puede ver los detalles de un grabador de configuración vinculado a un servicio mediante la consola o. AWS Config AWS CLI Para obtener más información, consulte Uso del registrador de configuración.	27 de noviembre de 2024

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config admite las siguientes reglas administradas: • appconfig-application-tagged • appconfig-configuration-profile-tagged • appconfig-environment-tagged • appconfig-extension-association-tagged • appmesh-gateway-route-tagged • appmesh-mesh-tagged • appmesh-route-tagged • appmesh-virtual-gateway-tagged • appmesh-virtual-node-tagged • appmesh-virtual-router-tagged • appmesh-virtual-service-tagged • evidently-launch-tagged • evidently-project-tagged • evidently-segment-tagged • frauddetector-entity-type-tagged • frauddetector-label-tagged • frauddetector-outcome-tagged	12 de noviembre de 2024

- frauddetector-variable-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Connect AWS AppConfig AWS CloudTrail, Amazon, Amazon DevOps Guru DataZone, Identity Store,, AWS Glue, Amazon Interactive Video Service (Amazon IVS) AWS IoT FleetWise AWS IoT Wireless, Amazon Logs, Amazon Observability Access AWS Payment Cryptography Manager, CloudWatch Amazon Relational Database Service (CloudWatch Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Simple Storage (S3), Amazon Scheduler y Amazon VPC Lattice. AWS IoT EventBridge AWS Systems Manager Para más información, consulte Políticas administradas de AWS para AWS Config.	8 de noviembre de 2024
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con la siguiente regla administrada: cognito-user-pool-advanced-security-enabled	6 de noviembre de 2024

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • active-mq-supported-version • rabbit-mq-supported-version • ec2- vpn-connection-log ging-enabled • appsync-cache-ct-e ncryption-en reposo • appsync-cache-ct-e ncryption-en tránsito • vpc-endpoint-enabled • efs-filesystem-ct-encrypted • redshift-cluster-subnet-gro up-multi-az • sns-topic-no-public-acceso • rabbit-mq-supported-version • kms-key-policy-no-acceso público • rds-mysql-instance-encrypte d-en tránsito • rds-postgres-instance-encry pted-en tránsito • rds-sql-server-logs-cloudwa tch • ec2- 2-check launch-te mplate-imdsv	21 de octubre de 2024

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para el PCI DSS 4.0 (excluye los tipos de recursos globales) • Prácticas operativas recomendadas para el PCI DSS 4.0 (incluye los tipos de recursos globales)	23 de septiembre de 2024
Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon OpenSearch Service Severless, Amazon AppStream,, AWS Backup AWS CloudTrail AWS Glue, EC2 Image Builder AWS IoT, Amazon Interactive Video Service (Amazon AWS Elemental MediaConnect IVS),, AWS Elemental MediaTailor, AWS HealthOmics y Amazon Scheduler . EventBridge Para más información, consulte Políticas administradas de AWS para AWS Config.	16 de septiembre de 2024

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • ec2- -gapped-vault resources-in-logically-air • ebs-resources-in-logically-air-gapped-vault • aurora-resources-in-logical ly-air-gapped-vault • efs-resources-in-logically-air-gapped-vault • s3- resources-in-logically-air -bóveda con huecos • storagegateway-resources-in-logically-air-gapped-vault • virtualmachine-resources-in-logically-air-gapped-vault	3 de septiembre de 2024
AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 1) • Prácticas operativas recomendadas para FedRAMP (nivel alto, parte 2)	27 de agosto de 2024

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • athena-workgroup-logging-enabled • codebuild-report-group-encr ypted-en reposo • cognito-user-pool-advanced-habilitado para la seguridad • datasync-task-logging-enabl ed • efs-automatic-backups-enabled • glue-job-logging-enabled • glue-ml-transform-encrypted -en reposo • kinesis-stream-backup-reten tion-comprobar • rds-aurora-postgresql-logs-a Cloudwatch • rds-postgresql-logs-to-vigilancia en la nube • workspaces-root-volume-encryption-habilitado • workspaces-user-volume-encryption-habilitado	22 de julio de 2024

Actualización de seguridad de IAM	Ahora, las políticas `AWSConfigServiceRolePolicy` y `AWS_ConfigRole` otorgan permisos adicionales para Amazon Elastic File System (Amazon EFS), Amazon Redshift y AWS Systems Manager para SAP. Para más información, consulte Políticas administradas de AWS para AWS Config.	17 de junio de 2024
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administradas: • cloudtrail-s3- bucket-public-access-prohibited • cloudtrail-s3- bucket-access-logging	8 de mayo de 2024
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con la siguiente regla administrada: iam-external-access-analyzer-enabled	2 de mayo de 2024

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • guardduty-malware-protectio n-enabled • guardduty-rds-protection-en abled • guardduty-s3-protection-ena bled • inspector-lambda-standard-s can-habilitado	26 de abril de 2024
AWS Config simplifica el análisis de uso con Amazon CloudWatch	Con esta versión, las CloudWatch métricas de Amazon para monitorea r el uso de AWS Config datos solo mostrarán el uso facturable. Esto significa que el uso no facturable ya no se mostrará ni en CloudWatch las estadísticas de Amazon emitidas a ni en la AWS Config AWS Config consola. Esto te permite validar la AWS Config configuración y el uso mediante CloudWatc h las métricas de Amazon y correlacionar el uso facturabl e con los costes asociados. Para obtener más información, consulte AWS Config Usage and Success Metrics.	26 de abril de 2024

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con la siguiente regla gestionada: iam-server-certificate-expiration-check	23 de abril de 2024
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • vpc-sg-port-restriction-com probar • cloudtrail-all-write-s3- data-event-check • cloudtrail-all-read-s3- data-event-check	17 de abril de 2024
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • guardduty-eks-protection-au dit-habilitado • guardduty-eks-protection-ru ntime-habilitado • guardduty-lambda-p rotection-enabled • inspector-ec2-scan-enabled • inspector-ecr-scan-enabled • inspector-lambda-code-scan-habilitado • redshift-unrestricted-port-access	16 de abril de 2024

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con la siguiente regla gestionada: efs-mount-target-public-accessible	20 de marzo de 2024
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • dms-neptune-iam-authorization-habilitado • dms-mongo-db-authentication-habilitado • dms-redis-tls-enabled • dax-tls-endpoint-encryption • eks-cluster-secrets-encrypted • kinesis-firehose-delivery-stream-encriptado • mq-cloudwatch-audit-log-habilitado • mq-cloudwatch-audit-log-habilitado • opensearch-primary-node-fault-tolerancia • sagemaker-endpoint-config-prod-recuento de instancias • service-catalog-shared-within-organización • transfer-family-server-no-ftp	26 de febrero de 2024

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales a Amazon Managed Service para Prometheus, CloudWatch Amazon, Amazon Cognito, Amazon, ElastiCache Amazon, (IAM), AWS Identity and Access Managemen t ,, FSx AWS Glue Amazon Redshift Serverless AWS Lambda AWS RAM, Amazon AI y Amazon Simple Notificat ion Service (SageMaker Amazon SNS). Para más información, consulte Políticas administradas de AWS para AWS Config.	22 de febrero de 2024
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con la siguiente regla administrada: s3- bucket-cross-region-replication - enabled	12 de febrero de 2024

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de AWS AppConfig recursos Amazon CloudWatch Evidently AWS Identity and Access Management (IAM), Amazon MemoryDB (MemoryDB), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Redshift y otros tipos de recursos. AWS Transfer Family Para obtener más información, consulte Tipos de recursos admitidos.	6 de febrero de 2024
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con la siguiente regla administrada: macie-auto-sensitive-data-discovery-check	29 de enero de 2024

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos Amazon AppStream, AWS Key Management Service (AWS KMS), Amazon Relational Database Service (Amazon RDS), Amazon Cognito, Amazon Elastic Compute Cloud (Amazon EC2), EC2 Image Builder, Amazon Quick AWS Ground Station AWS Mainframe Modernization, Amazon Redshift y los tipos de recursos. AWS Systems Manager Para obtener más información, consulte Tipos de recursos admitidos.	3 de enero de 2024

Los límites de servicio aumentan según el número máximo de reglas por región y cuenta AWS Config	Con esta versión, AWS Config admite 1000 AWS Config reglas por AWS región y cuenta. Este aumento se aplica al total de todas las reglas implementadas, incluidas las reglas AWS Config administradas, las reglas AWS Config personali zadas, los paquetes de AWS Config conformidad, AWS Security Hub CSPM los controles, AWS Firewall Manager las políticas y los planes de AWS Backup respaldo por región y cuenta. Para obtener más información, consulte Límites de servicio.	19 de diciembre de 2023

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • s3- meets-restore-time-target • ebs-meets-restore-time-objetivo • ec2- meets-restore-time-target • rds-meets-restore-time-objetivo • efs-meets-restore-time-objetivo • fsx-meets-restore-time-objetivo • aurora-meets-restore-time-objetivo • dynamodb-meets-restore-time-objetivo	19 de diciembre de 2023

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para AWS AppConfig Amazon Managed Service for Prometheus AWS Database Migration Service ,AWS DMS(), () IAM, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management(Amazon MSK) AWS Organizations, Amazon Logs y CloudWatch Amazon Simple Storage Service (Amazon S3). Para más información, consulte Políticas administradas de AWS para AWS Config.	5 de diciembre de 2023

Versión preliminar: procesador de consultas en lenguaje natural para consultas avanzadas	Con esta versión, puede utilizar el procesador de consultas en lenguaje natural para consultas avanzadas, que utiliza capacidades de inteligencia artificial generativa (IA generativa) que le permiten hacer preguntas en un lenguaje sencillo y convertirlas en un formato de ready-to-use consulta. Con el procesador de consultas en lenguaje natural, puede realizar consultas en su organización Cuenta de AWS o en toda la organización AWS . Para obtener más información, consulte Procesador de consultas en lenguaje natural para consultas avanzadas.	26 de noviembre de 2023

Registro periódico	Con esta versión, AWS Config admite la grabación periódica. El registro periódico le permite capturar los cambios de configuración más recientes de sus recursos durante un período de tiempo fijo. Ahora puede establecer la frecuenci a predeterminada del registrad or de configuración en Diaria, lo que le permitirá recibir un elemento de configura ción (CI) que represente el estado más reciente de sus recursos durante las últimas 24 horas, solo si es diferente del CI anterior registrado. La AWS Config consola también presenta una nueva experiencia de estrategia de grabación, en la que también se puede anular la frecuenci a de grabación para tipos de recursos específicos o excluir tipos de recursos específicos de la grabación. Esto puede ayudar a que la configuración se adapte a sus requisitos detallados. Se añaden los siguientes tipos de datos: • RecordingMode • RecordingModeOverride	26 de noviembre de 2023

Se han actualizado los siguientes tipos de datos:

- PutConfigurationRecorder
- ConfigurationRecorder
- BaseConfigurationItem
- ConfigurationItem

Se han actualizado las siguientes páginas de la guía para desarrolladores:

- Recoding AWS Resources
- Configuración AWS Config con la AWS Config consola | Configuración con un solo clic
- Configuración AWS Config con la AWS Config consola | Configuración manual
- Configuración AWS Config con la AWS CLI

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Cognito, Amazon Connect, Amazon EMR, Amazon MemoryDB AWS Ground Station, AWS Mainframe Modernization Amazon Quick AWS Organizations, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53 y. AWS Service Catalog AWS Transfer Family Las políticas `AWSConfigServiceRolePolicy` y `AWS_ConfigRole` ahora también añaden identificadores de seguridad (SID) para `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , `AWSConfigSLRApiGatewayStatementID` , y la política de `AWSConfigServiceRolePolicy` . Para más información, consulte Políticas administr	17 de noviembre de 2023

	adas de AWS para AWS Config.	
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • acm-pca-root-ca-deshabilita do • dynamodb-table-deletion-protection-habilitado • ec2- -habilitado client-vpn-connection-log • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-confi gurado • fsx-openzfs-copy-tags-habil itado • fsx-lustre-copy-tags-a copias de seguridad • msk-enhanced-monitoring-enabled • mq-auto-minor-version-habil itada para la actualización • neptune-cluster-multi-az-ha bilitado • opensearch-update-check • s3- -solo access-point-in-vpc • s3- -bloques access-point-public-access • s3- bucket-mfa-delete-enabled	9 de noviembre de 2023

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos AWS Identity and Access Management (IAM), AWS Network Manager, AWS Private Certificate Authority (AWS Private CA), Amazon Connect AWS App Mesh, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) AWS IoT, Amazon Managed Streaming AWS IoT TwinMaker for Apache Kafka Connect (Amazon MSK Connect) y recurso tipos. AWS Lambda Explorador de recursos de AWS Para obtener más información, consulte Tipos de recursos admitidos.	3 de noviembre de 2023
AWS Config admite nuevos paquetes de conformidad	Con esta versión, se AWS Config actualiza el siguiente paquete de conformidad: Mejores prácticas operativas para el BNM T RMi	26 de octubre de 2023

Paneles de cumplimiento e inventario para agregadores	Con esta versión, AWS Config agrega una página de panel de cumplimiento y una página de panel de inventario a la vista agregada de la AWS Config consola. En la página del panel de cumplimiento, puede ver paneles automatizados con widgets que resumen la información sobre el cumplimiento de los recursos en su agregador, como los 10 principales tipos de recursos por recursos no conformes, los 10 principales paquetes de conformidad de nivel de cuenta por normas no conformes, etc. En la página del panel de inventario, puede ver paneles automatizados con widgets que resumen la información sobre los datos de configura ción de los recursos en su agregador, como los 10 principales tipos de recursos por recuento de recursos, las 10 principales cuentas por recuento de recursos, etc. Para obtener información sobre los gráficos, consulte Panel de cumplimiento y Panel de inventario.	23 de octubre de 2023

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Connect AWS Private CA AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon Evidentemente, CloudWatch Amazon Managed Grafana, Amazon, GuardDuty Amazon AWS IoT Inspector AWS IoT TwinMaker,, Amazon Managed Streaming for Apache Kafka (Amazon AWS Lambda MSK AWS Network Manager) AWS Organizations,, y Amazon AI. SageMaker Para más información, consulte Políticas administradas de AWS para AWS Config.	4 de octubre de 2023

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos AWS IoT AWS IoT TwinMaker tipos de AWS IoT Wireless recursos Amazon Personalize Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon SageMaker AI, AWS CodeBuild Amazon y Amazon AppStream Inspector . Para obtener más informaci ón, consulte Tipos de recursos admitidos.	4 de octubre de 2023

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • docdb-cluster-deletion-prot ection-habilitado • docdb-cluster-audit-logging-habilitado • docdb-cluster-snapshot-publ ic-prohibido • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-veri ficación de actualizaciones • dms-replication-task-target db-registro • dms-replication-task-source db-registro • dms-endpoint-ssl-configured • custom-eventbus-policy-atta ched • global-endpoint-event-repli cation-habilitado • ruta 53- query-logging-enab led • rds-aurora-mysql-audit-habi litado para el registro • rds-cluster-auto-minor-vers ion-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-e nabled	21 de septiembre de 2023

	• wafv2- rulegroup-logging-enabled • msk-in-cluster-node-require-tls	
AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config actualiza los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para Amazon S3 • Prácticas operativas recomendadas para EC2	8 de septiembre de 2023
Actualización de seguridad de IAM	Ahora, la política `AWSConfigServiceRolePolicy` elimina los permisos para AWS Systems Manager (Systems Manager). Para más información, consulte Políticas administradas de AWS para AWS Config.	6 de septiembre de 2023

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizar esta versión AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon CodeGuru Profiler AWS Elemental MediaConnect AWS Transfer Family,,, Amazon Managed Service for Prometheus AWS Batch y AWS Cloud Map. Amazon Route 53 Resolver Para obtener más información, consulte Tipos de recursos admitidos.	6 de septiembre de 2023

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • athena-workgroup-e ncrypted-at-descansar • neptune-cluster-iam-databas e-autenticación • neptune-cluster-copy-tags-t o-snapshot-enabled • neptune-cluster-cloudwatch-log-habilitado para la exportación • neptune-cluster-deletion-pr otection-habilitado • neptune-cluster-snapshot-en crypted • neptune-cluster-backup-rete ntion-comprobar • neptune-cluster-encrypted • neptune-cluster-snapshot-pu blic-prohibido • docdb-cluster-backup-retent ion-comprobar • docdb-cluster-encrypted • rds-cluster-encrypted-at-de scansar	10 de agosto de 2023

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos Amazon AWS Amplify AppIntegrations, Amazon Athena AWS App Mesh, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidentemente, Amazon Forecast, CloudWatch ,,, Amazon Managed Streaming for Apache Kafka (Amazon MSK) AWS Elemental MediaTailor, Amazon Personalize, Amazon Pinpoint y tipos de recursos. AWS IoT Greengrass Version 2 AWS Ground Station AWS Elemental MediaConvert AWS Resilience Hub Para obtener más información, consulte Tipos de recursos admitidos.	3 de agosto de 2023

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Managed Workflows for AWS App Mesh, Amazon WorkSpaces Applications AWS CloudFormation, Amazon CloudFront AWS CodeArtifact AWS CodeBuild , Amazon Connect, Amazon AWS Glue, AWS Identity and Access Management (IAM) GuardDuty, Amazon Inspector,, AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie AWS Elemental MediaConnect,,,, Amazon Route 53 AWS Network Manager AWS Organizations Explorador de recursos de AWS, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS) y Amazon EC2 Systems Manager (SSM). Para más información, consulte Políticas administradas de AWS para AWS Config.	28 de julio de 2023

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos Amazon Kinesis, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC), Amazon Kendra, Amazon Connect,, tipos de recursos AWS CloudFormation, AWS AppConfig y (). AWS App Mesh AWS App Runner AWS Database Migration Service A WS DMS Para obtener más información, consulte Tipos de recursos admitidos.	10 de julio de 2023
Los límites de servicio aumentan para los paquetes de conformidad de la organización	Con esta versión, AWS Config admite 350 AWS Config reglas por región y cuenta en todos los paquetes de conformid ad y 350 reglas organizativas por organización. AWS Config Para obtener más información, consulte Límites de servicio.	13 de junio de 2023

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales a Amazon Managed Workflows para Amazon Connect AWS Amplify AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena,,,, Amazon, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evident, Amazon Forecast, ,,,, (IAM), Amazon Transmisión AWS Identity and Access Management gestionada para Apache Kafka (Amazon MSK) AWS Organizations, AWS IoT Greengrass AWS Ground Station Amazon Lightsail, Amazon Logs, CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon Quick, AWS Migration Hub Refactor Spaces Amazon Simple Storage Service (Amazon S3), Amazon AI y.	13 de junio de 2023

	SageMaker AWS Transfer Family Para más información, consulte Políticas administradas de AWS para AWS Config.

AWS Config Exclusiones de registro por tipo de recurso	Con esta versión, puede AWS Config excluir tipos específicos de AWS recur sos del seguimiento del inventario y la supervisión del cumplimiento y, al mismo tiempo, realizar un seguimien to de todos los demás tipos de recursos compatibles disponibles actualmente AWS Config, incluidos los que se añadirán en el futuro. Puede usar esta característica para concentrarse en los recursos críticos que están sujetos a los estándares de cumplimiento y gobernanza. Las actualizaciones de la API para la grabadora de configuración y el grupo de grabación son compatibles con versiones anteriores, lo que significa que funcionan con versiones anteriores de la PutConfigurationRecorderAPI. Puede seguir gestionando los tipos de recursos que se registran exactamente de la misma forma que antes, sin necesidad de utilizar los actualizados o los nuevos APIs. Se añaden los siguientes tipos de datos:	9 de junio de 2023

- RecordingStrategy
- ExclusionByResourceTypes

Se han actualizado los siguientes tipos de datos:

- PutConfigurationRecorder
- ConfigurationRecorder
- RecordingGroup

Se ha actualizado la siguiente página de la guía para desarrolladores:

- Selección de los recursos que se va a registrar

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos Amazon Elastic Container Service (Amazon ECS), Amazon Keyspaces (para Apache Cassandra) (Amazon Keyspaces),,,, Amazon WorkSpaces Applicati ons AWS Signer AWS Amplify AWS App Mesh, AWS App Runner Amazon Elastic Compute Cloud (Amazon EC2) AWS CodeArtif act, Amazon CloudWatch Evident, Amazon Forecast (AWS Identity and Access Management IAM), Tipos de recursos de Amazon Pinpoint, Amazon AI y Amazon Data Firehose. SageMaker AWS Transfer Family Para obtener más información, consulte Tipos de recursos admitidos.	5 de junio de 2023

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • cloudfront-s3- origin-access-control-enabled • custom-schema-registry-policy-adjunto • ec2- -todos client-vpn-not-authorize • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-habilitado para la actualización • mq-cloudwatch-audit-logging-habilitado • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-habilitado para el registro	10 de mayo de 2023

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos Amazon Route 53 Resolver Amazon Elastic Compute Cloud (Amazon EC2) AWS IoT , Wireless,, AWS Network Manager, Amazon AWS Device Farm AWS Ground Station, Amazon Redshift, AppFlow Amazon Pinpoint,, EC2 Image Builder AWS IoT AWS AppConfig, Amazon, Amazon Runtime SageMaker , AWS Panorama Amazon ECR y tipos de recursos. CloudWatch AWS Audit Manager Para obtener más información, consulte Tipos de recursos admitidos.	5 de mayo de 2023
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en`AWS::NetworkFirewall::TLSInspectionConfiguration` . Para obtener más información, consulte Tipos de recursos admitidos.	1 de mayo de 2023

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Managed Workflows para AWS Amplify AWS App Mesh, AWS App Runner, Amazon CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, SageMaker Amazon AWS Transfer Family AI, Amazon AWS Migration Hub Pinpoint AWS , Resilience Hub, Amazon CloudWatch, AWS Directory Service y. AWS WAF Para más información, consulte Políticas administradas de AWS para AWS Config.	13 de abril de 2023

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • elasticache-auto-minor-vers ion-verificación de actualiza ciones • elasticache-repl-grp-auto-h abilitado para la conmutaci ón por error • elasticache-repl-grp-encryp ted-en reposo • elasticache-repl-grp-encryp ted-en tránsito • elasticache-repl-grp-redis- habilitado para la autentica ción • elasticache-subnet-group-ch eck • cloudfront-s3- origin-non- existent-bucket	10 de abril de 2023
Los límites de servicio aumentan para los paquetes de conformidad de la organización	Con esta versión, AWS Config admite 350 AWS Config reglas por cuenta en todos los paquetes de conformidad de la organización. Para obtener más información, consulte Límites de servicio.	3 de abril de 2023

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-descansar	3 de abril de 2023

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de las nuevas WorkSpaces aplicaciones de Amazon, AWS Auto Scaling, Amazon Connect, Amazon Elastic Compute Cloud EventBridge, Amazon HealthLake, Kinesis video stream, Lookout for Vision AWS IoT TwinMaker, Network Manager, Amazon Pinpoint, Amazon Application Recovery Controller (ARC) y tipos de recursos. AWS RoboMaker Para obtener más informaci ón, consulte Tipos de recursos admitidos.	3 de abril de 2023

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Managed Workflows for Amazon AppFlow AWS App Runner, Amazon WorkSpaces Applications, Amazon AWS CloudFormation, Amazon CloudFront,, CloudWatch, AWS CodeArtifact AWS CodeCommit AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidentemente, CloudWatch Amazon Forecast,, (AWS IoT IAM), AWS Ground Station Amazon AWS Identity and Access Management MemoryDB, Amazon AWS Network Manager Pinpoint,,, Amazon Relational Database Service Amazon (Amazon RDS) AWS Panorama, Amazon Redshift y Amazon AI. SageMaker Para más información, consulte Políticas administradas de AWS para AWS Config.	30 de marzo de 2023

Actualización de seguridad de IAM	Ahora, la política de `AWSConfigServiceRolePolicy` y la política de `AWS_ConfigRole` otorgan permisos adicionales a AWS Audit Manager. Para más información, consulte Políticas administradas de AWS para AWS Config.	3 de marzo de 2023
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon AWS Elemental MediaPackage EventBridge AWS IoT,, (Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Lookout for Metrics, Amazon Lex AWS Device Farm, CodeGuru , Amazon Reviewer y AWS Budgets otros tipos de recursos. Amazon Route 53 Resolver AWS RoboMaker Para obtener más información, consulte Tipos de recursos admitidos.	2 de marzo de 2023

Actualización de seguridad de IAM	AWS Config ahora realiza un seguimiento de los cambios en la política`AWSConfigMultiAccountSetupPolicy` . Para más información, consulte Políticas administradas de AWS para AWS Config.	27 de febrero de 2023
AWS Config Cobertura de recursos por región y disponibilidad	Con esta versión, AWS Config proporciona información sobre la región para cada tipo de recurso compatible. Para obtener información sobre los tipos de recursos admitidos en determinadas regiones, consulte Cobertura de recursos según la disponibilidad por región.	20 de febrero de 2023

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos Amazon Interactive Video Service (Amazon IVS), Amazon Simple Storage Service (Amazon AWS Glue S3), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon AWS IoT Relational Database Service (Amazon RDS) y Managed Service for Apache Flat Tipos de recursos de enlace. Para obtener más información, consulte Tipos de recursos admitidos.	7 de febrero de 2023

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Managed Workflows for Apache Airflow, AWS IoT Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), AWS Device Farm Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM), Amazon y Amazon Logs. GuardDuty CloudWatch Para más información, consulte Políticas administradas de AWS para AWS Config.	1 de febrero de 2023
Actualización de seguridad de IAM	Como práctica recomendada de seguridad, ahora la política de `ConfigConformsServiceRolePolicy` elimina los permisos amplios en el nivel de los recursos para `config:DescribeConfigRules` . Para más información, consulte Políticas administradas de AWS para AWS Config.	12 de enero de 2023

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Managed Service for Prometheus AWS Audit Manager,,, (), AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2 AWS Glue) AWS Directory Service,, Amazon Lightsail,, Amazon Quick AWS IoT, AWS Elemental MediaPackage Amazon AWS Network Manager Application Recovery Controller (ARC), AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) y Amazon Timestre3) Amazon Timestream. Para más información, consulte Políticas administradas de AWS para AWS Config.	10 de enero de 2023

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los nuevos Amazon MQ,, AWS AppConfig , AWS Cloud9 Amazon EventBridge Schemas, Amazon Fraud Detector,, Amazon AWS IoT Analytics Lightsail AWS IoT, AWS Elemental MediaPackage (MediaPackage), Amazon Application Recovery Controller (ARC) y tipos de recursos. AWS Resilience Hub AWS Transfer Family Para obtener más información, consulte Tipos de recursos admitidos.	5 de enero de 2023
AWS Config regule la cobertura de los recursos	En esta versión, AWS Config muestra la cobertura de los tipos de recursos para un mayor número de reglas AWS Config administradas.	21 de diciembre de 2022
AWS Config capacidad de detección de reglas	En esta versión, AWS Config admite páginas para la lista de reglas AWS Config administradas por modo de evaluación, la lista de reglas AWS Config administradas por tipo de activación y la lista de reglas AWS Config administradas por región de disponibilidad.	21 de diciembre de 2022

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config actualiza los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para K-ISMS • Prácticas operativas recomendadas para NIST 800 171 • Prácticas operativas recomendadas para el PCI DSS 3.2.1 • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Alto • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Medio • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Bajo • Prácticas operativas recomendadas para el NZISM • Prácticas operativas recomendadas para el NIST 800-53 rev 5	19 de diciembre de 2022

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • api-gwv2- access-logs-enabled • api-gwv2- authorization-type -configured • cloudfront-security-policy-check • ec2- -deshabilitado launch-template-public-ip • elastic-beanstalk-logs-to-c loudwatch • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-control de acceso • security-account-informatio n-provided • storagegateway-resources-protected-by-plan de respaldo • wafv2- rulegroup-not-empty • wafv2- webacl-not-empty	9 de diciembre de 2022

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon CloudWatch RUM GuardDuty , Amazon, Amazon, Amazon Simple Email Service (Amazon SES) AWS Backup AWS DataSync,, AWS Fault Injection Service y AWS FIS(). EventBridge Para obtener más información, consulte Tipos de recursos admitidos.	9 de diciembre de 2022

AWS Config Cumplimiento proactivo	Con esta versión, AWS Config permite comprobar de forma proactiva el cumplimiento de AWS Config las normas antes del aprovisionamiento de recursos. Esto le permite evaluar los ajustes de configuración de sus recursos antes de crearlos o cargarlos. Úselo AWS Config para realizar un seguimiento de los cambios de configuración realizados en sus recursos, ya sea antes o después del aprovisionamiento, y comprobar si los recursos coinciden con las configuraciones deseadas. Se añaden los siguientes tipos de datos: • GetResourceEvaluationSummary • StartResourceEvaluation • ListResourceEvaluations Se han actualizado los siguientes tipos de datos: • DescribeConfigRulesFilters • GetComplianceDetailsByResource • EvaluationResultQualifier • EvaluationModeConfiguration	28 de noviembre de 2022

Se han actualizado las siguientes páginas de la guía para desarrolladores:

- Componentes de una regla AWS Config
- Modo de evaluación y tipos de activadores de AWS Config las reglas
- AWS Config Reglas administradas
- Reglas personalizadas de AWS Config
- Administrar sus AWS Config reglas

La detección de desviaciones como elemento de configuración (CI) para el registrador AWS Config de configuración	Con esta versión, AWS Config realiza un seguimiento de todos los cambios realizados en la grabadora de configuración para indicar si el estado de la grabadora de configuración difiere o se ha desviado de su estado anterior; por ejemplo, si hay actualizaciones en los tipos de recursos que ha habilitado AWS Config para rastrear, si ha detenido o iniciado la grabadora de configuración o si ha eliminado o desinstalado la grabadora de configuración. El tipo de `AWS::Config::ConfigurationRecorder` recurso es un tipo de recurso del sistema AWS Config y el registro de este tipo de recurso está habilitado de forma predeterminada en todas las regiones compatibles. El registro de este tipo de recurso `AWS::Config::ConfigurationRecorder` no tiene costo adicional. Para obtener más información, consulte Administración del registrador de configuración.	18 de noviembre de 2022

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de AWS Cloud Map recursos AWS IoT Events, EC2 Image Builder AWS DataSync, AWS Glue, Amazon Application Recovery Controller (ARC) y Amazon Elastic Container Registry (Amazon ECR). Para obtener más información, consulte Tipos de recursos admitidos.	8 de noviembre de 2022
Actualización de seguridad de IAM	Ahora, la política de `AWSConfigServiceRolePolicy` y la política de `AWS_ConfigRole` otorgan permisos adicionales a AWS CloudFormation. Para más información, consulte Políticas administradas de AWS para AWS Config.	7 de noviembre de 2022

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para los Servicios de Información de la Justicia Criminal (CJIS) • Mejores prácticas de seguridad para Amazon SageMaker AI • Prácticas de seguridad recomendadas para Amazon Elastic Container Registry Se han actualizado los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para MAS TRMG • Prácticas operativas recomendadas para el NCSC Cyber Assesment Framework • Prácticas operativas recomendadas para los NCSC Cloud Security Principles	27 de octubre de 2022

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow, AWS AppConfig Amazon Keyspaces, Amazon AWS Amplify, Amazon Connect, Amazon CloudWatch Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, EventBridge Amazon AWS Fault Injection Service, Amazon Servidores, FSx Amazon Location AWS IoT Service GameLift , Amazon Lex, Amazon Lightsail, Amazon Pinpoint, Amazon Quick, Amazon OpsWorks AWS Panorama AWS Resource Access Manager Relational Database Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker Amazon Grupos de recursos de AWS Route 53, Amazon Simple Storage Service (Amazon S3) y. AWS Cloud Map AWS	19 de octubre de 2022

	Security Token Service Para más información, consulte Políticas administradas de AWS para AWS Config.	
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Email Service (Amazon AWS AppConfig SES) AWS Cloud Map y tipos de recursos. AWS DataSync Para obtener más informaci ón, consulte Tipos de recursos admitidos.	6 de octubre de 2022
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los nuevos tipos de AWS DataSync recursos de Amazon GuardDuty AWS AppSync AWS Cloud Map, Amazon SageMaker AI y. Para obtener más información, consulte Tipos de recursos admitidos.	4 de octubre de 2022
AWS Config admite el nuevo paquete de conformidad	Con esta versión, se AWS Config actualiza el paquete de conformidad con las mejores prácticas operativas para el CSP de SWIFT.	4 de octubre de 2022

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para la CMMC 2.0 de nivel 1 • Prácticas operativas recomendadas para la CMMC 2.0 de nivel 2 Se han actualizado los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para Amazon API Gateway • Mejores prácticas operativas para el pilar de AWS confiabilidad de un marco bien diseñado • Mejores prácticas operativas para el pilar de seguridad de AWS Well-Architected Framework • Prácticas operativas recomendadas para la CMMC de nivel 1 • Prácticas operativas recomendadas para la CMMC de nivel 2	30 de septiembre de 2022

	• Prácticas operativas recomendadas para la CMMC de nivel 3 • Prácticas operativas recomendadas para la CMMC de nivel 4 • Prácticas operativas recomendadas para la CMMC de nivel 5 • Prácticas operativas recomendadas para FFIEC • Prácticas operativas recomendadas para el FedRAMP (bajo) • Prácticas operativas recomendadas para MAS Notice 655 • Prácticas operativas recomendadas para NBC TRMG • Prácticas operativas recomendadas para NIST 800 172	
Actualización de seguridad de IAM	Ahora, la política de `AWSConfigServiceRolePolicy` y la política de `AWS_ConfigRole` otorgan permisos adicionales a AWS Glue. Para más información, consulte Políticas administradas de AWS para AWS Config.	14 de septiembre de 2022

AWS Config admite el nuevo paquete de conformidad	Con esta versión, AWS Config es compatible con el paquete de conformidad con las mejores prácticas operativas para el CSP de SWIFT.	9 de septiembre de 2022

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon AppFlow, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas, Amazon Fraud Detector Detector, EventBridge Amazon Servers, Amazon FinSpace Amazon Interactive Video Service (Amazon IVS) GameLift , Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble Pinpoint, Amazon Quick, StudioAmazon Amazon Application Recovery Controller (ARC), Amazon Simple Storage	7 de septiembre de 2022

Service (Amazon S3) Simple Email Service (Amazon SES), Amazon Route 53 Resolver Amazon Simple Email Service (Amazon S3), Amazon Timestream,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker , AWS Lake Formation AWS License Manager, AWS Resilience Hub, AWS Signer, y AWS Transfer Family. Para más información, consulte Políticas administradas de AWS para AWS Config.

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Mejores prácticas operativas para Amazon CloudWatch • Catálogo de controles de cumplimiento de las prácticas operativas recomendadas para la computación en nube en Alemania (C5) • Prácticas operativas recomendadas para IRS 1075 Se han actualizado los siguientes paquetes de conformidad: • AWS Paquete de conformidad con las barandillas Control Tower Detective • Prácticas operativas recomendadas para CISA Cyber Essentials • Guía de mejores prácticas operativas para la ciberseguridad de ENISA para SMEs • Prácticas operativas recomendadas para la FDA Título 21 CFR Parte 11	31 de agosto de 2022

	• Prácticas operativas recomendadas para FedRAMP (moderadas) • Prácticas operativas recomendadas para la seguridad de HIPAA • Prácticas operativas recomendadas para el NIST Privacy Framework v1.0 • Prácticas operativas recomendadas para NYDFS 23 • Mejores prácticas operativas para el marco de ciberseguridad del RBI para UCBs • Prácticas operativas recomendadas para RBI MD-ITF	
Cómo empezar con las AWS Config actualizaciones del paquete de conformidad personalizadas	Con esta versión, se AWS Config actualizan las páginas de introducción AWS Config y configuración de la consola e incorpora una página de configuración manual y una página de configuración manual AWS Config conun solo clic. AWS Config también actualiza la página del paquete de conformidad personalizado con un tutorial sobre cómo crear un archivo YAML del paquete de conformidad desde cero.	25 de agosto de 2022

AWS Systems Manager Integración del documento (documento SSM) con los paquetes de conformidad	En esta versión, puede crear una plantilla de paquete de conformidad con un documento SSM. Para obtener más información sobre los documentos SSM, consulte Documentos de AWS Systems Manager en la Guía del usuario de AWS Systems Manager . Se han actualizado los siguientes tipos de datos: • PutConformancePack • ConformancePackDetail • Detalles de la plantilla SSMDocument Se han actualizado las siguientes páginas de la guía para desarrolladores: • Implementación de un paquete de conformidad mediante la consola AWS Config • Implementación de un paquete de conformidad mediante la interfaz de AWS línea de comandos	24 de agosto de 2022

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Simple Email Service (Amazon SES) AWS DataSync, AWS Cloud Map y. Para más información, consulte Políticas administradas de AWS para AWS Config.	22 de agosto de 2022
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon Athena, Amazon Detective, Amazon SageMaker AI, AWS Database Migration Service Amazon Route 53, AWS Key Management Service (AWS KMS) AWS Glue,, () y Amazon Simple Email Service (Amazon SES).AWS DMS Para obtener más información, consulte Tipos de recursos admitidos.	16 de agosto de 2022

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config actualiza los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para NIST 1800 25 • Prácticas operativas recomendadas para NIST 800 181 • Prácticas operativas recomendadas para cargas de trabajo estándar de ABS CCIG 2.0 • Prácticas operativas recomendadas para cargas de trabajo de material de ABS CCIG 2.0 • Prácticas operativas recomendadas para ACSC Essential 8 • Prácticas operativas recomendadas para ACSC ISM • Prácticas operativas recomendadas para APRA CPG 234 • Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4, nivel 1 • Benchmark v1.4, nivel 2, de mejores prácticas operativa s para AWS las fundaciones de la CEI	1 de agosto de 2022

- Mejores prácticas operativas para BNM T RMi
- Prácticas operativas recomendadas para el NIST CSF

Puntuación de conformidad para los paquetes de conformidad	En esta versión, se AWS Config presenta la puntuación de conformidad de los paquetes de conformidad, que le proporciona una visión general del estado de conformidad de sus paquetes de conformidad. Puede utilizarla para identificar, investigar y comprender el nivel de conformidad de sus paquetes de conformidad. La puntuación de conformidad es el porcentaje del número de combinaciones de reglas y recursos conformes en un paquete de conformidad en comparación con el número total de combinaciones posibles de reglas y recursos en el paquete de conformidad. Se han actualizado los siguientes tipos de datos: • ListConformancePackComplianceScores • ConformancePackComplianceScore Se han actualizado las siguientes páginas de la guía para desarrolladores: • Visualización del panel AWS Config	26 de julio de 2022

	• Visualización de los datos de conformidad en el panel de paquetes de conformidad • Administración de paquetes de conformidad (API)	
Actualización de seguridad de IAM	La `ConfigConformsServiceRolePolicy` política ahora otorga permiso para publicar puntos de datos métricos en Amazon CloudWatch. Para más información, consulte Políticas administradas de AWS para AWS Config.	25 de julio de 2022

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon ElastiCache EventBridge, Amazon Managed Service for Apache Flink FSx, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon Quick, Amazon Rekognition, Amazon Simple Storage Service (AWS RoboMaker Amazon S3) (Amazon S3), Amazon Simple Email Service (Amazon SES),,,,,,, (Centro de identidad de IAM AWS Amplify) AWS AppConfig, EC2 Image AWS Firewall Manager Builder AWS Glue, AWS AppSync AWS Billing Conductor AWS DataSync AWS IAM Identity Center y Elastic Load Balancing. Para más información, consulte Políticas administradas de AWS para AWS Config.	15 de julio de 2022

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon Elastic Compute Cloud (Amazon EC2). Para obtener más información, consulte Tipos de recursos admitidos.	8 de julio de 2022
AWS Config admite un nuevo tipo de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de AWS Global Accelerat or recursos. Para obtener más información, consulte Tipos de recursos admitidos.	5 de julio de 2022
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • autoscaling-launch-template • ecs-task-definition-log-con figuración • ecs-awsvpc-networking-enabled	1 de julio de 2022

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para el Perfil medio de control de la nube del Centro Canadiense de Ciberseguridad (CCCS) • Prácticas operativas recomendadas para la Ley Gramm Leach Bliley (GLBA) • Prácticas operativas recomendadas para el anexo 11 de la UE de GxP • Prácticas de seguridad recomendadas para Amazon Elastic Kubernetes Service (Amazon EKS) • Prácticas de seguridad recomendadas para Amazon Relational Database Service (Amazon RDS) • Prácticas recomendadas de seguridad para AWS Lambda Se han actualizado los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para IA y ML	30 de junio de 2022

	• Prácticas operativas recomendadas para Amazon DynamoDB • Mejores prácticas operativas para CIS Critical Security Controls v8 IG1 • Mejores prácticas operativas para los controles de seguridad críticos del CIS, versión 8 IG2 • Mejores prácticas operativas para los controles de seguridad críticos del CIS, versión 8 IG3 • Prácticas operativas recomendadas para la seguridad de HIPAA • Prácticas operativas recomendadas para el NIST 800-53 rev 5 • Prácticas operativas recomendadas para el NIST CSF	
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon SageMaker AI. Para obtener más información, consulte Tipos de recursos admitidos.	29 de junio de 2022

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Route 53 WorkSpaces, Amazon AWS Batch, AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), AWS Database Migration Service (AWS DMS) y Elastic AWS Step Functions Load Balancing. Para obtener más información, consulte Tipos de recursos admitidos.	14 de junio de 2022

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • aurora-last-backup-recovery -punto creado • dynamodb-last-backup-recovery-punto creado • ebs-last-backup-recovery-pu nto creado • ec2- -creado last-backup-recovery-point • efs-last-backup-recovery-pu nto creado • fsx-last-backup-recovery-pu nto creado • rds-last-backup-recovery-pu nto creado • s3- -creado last-backup-recovery-point • storagegateway-last-backup-recovery-punto creado • virtualmachine-last-backup-recovery-punto creado	13 de junio de 2022

AWS Config Integración con AWS Security Hub CSPM	Con esta versión, puede ver los resultados de las evaluaciones de reglas AWS Config gestionadas y personalizadas como hallazgos en AWS Security Hub CSPM. Security Hub CSPM transforma las evaluaciones de reglas en hallazgos, que proporcionan más información sobre los recursos afectados, como el nombre del recurso de Amazon (ARN) y la fecha de creación. Estos resultados se pueden ver junto con otros resultados del CSPM de Security Hub, lo que proporciona una visión general completa de la posición de seguridad. Para obtener más información, consulte Envío de evaluaciones de reglas a Security Hub (CSPM).	7 de junio de 2022

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para Amazon Athena, Amazon Detective, Amazon GuardDuty, Amazon Macie, Amazon Simple Email Service (Amazon AWS Glue SES) AWS Resource Access Manager ,,AWS RAM() y. AWS IAM Identity Center Para más información, consulte Políticas administradas de AWS para AWS Config.	31 de mayo de 2022

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Prácticas de seguridad recomendadas para Amazon Elastic Container Service (Amazon ECS) • Prácticas de seguridad recomendadas para Amazon Elastic File System (Amazon EFS) • Mejores prácticas de seguridad para Amazon CloudFront • Mejores prácticas de seguridad para AWS Auto Scaling • Mejores prácticas de seguridad para AWS Network Firewall • Mejores prácticas de seguridad para AWS Secrets Manager	31 de mayo de 2022
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los nuevos tipos de AWS Step Functions recursos y SageMaker IA de Amazon. Para obtener más información, consulte Tipos de recursos admitidos.	26 de mayo de 2022

AWS Config admite el nuevo paquete de conformidad	Con esta versión, se AWS Config actualiza el paquete de conformidad con las mejores prácticas operativas para el NERC CIP BCSI.	20 de mayo de 2022
Componentes de una regla AWS Config	En esta versión, se AWS Config presenta una página sobre los componentes de una AWS Config regla. La página analiza la estructura de las definiciones de reglas, los metadatos de las reglas y las mejores prácticas sobre cómo escribir reglas con Python mediante el kit de desarrollo de AWS Config reglas (RDK) y la biblioteca del kit de desarroll o de AWS Config reglas (RDKlib).	9 de mayo de 2022
Los límites de servicio aumentan para los paquetes de conformidad de la organización	Con esta versión, AWS Config admite 180 AWS Config reglas por cuenta en todos los paquetes de conformidad de la organización. Para obtener más información, consulte Límites de servicio.	6 de mayo de 2022

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Mejores prácticas de seguridad para Amazon OpenSearch Service • Prácticas de seguridad recomendadas para Amazon Redshift • Mejores prácticas de seguridad para AWS CloudTrail • Mejores prácticas de seguridad para AWS CodeBuild • Mejores prácticas de seguridad para AWS WAF	29 de abril de 2022
AWS Config actualiza la regla gestionada	Con esta versión, AWS Config es compatible con la regla gestionada resources-protected-by-backuppor el plan s3.	11 de abril de 2022

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos adicionales para obtener información sobre todo el almacén de datos de AWS CloudTrail eventos (EDS) o sobre uno específico, obtener información sobre todos o un AWS CloudFormation recurso específico, obtener una lista de un grupo de parámetros o un grupo de subredes de DynamoDB Accelerator (DAX), obtener información AWS Database Migration Service sobre AWS DMS() las tareas de replicación de su cuenta en la región actual a la que se está accediendo y obtener una lista de todas las políticas de un tipo específico. AWS Organizations Para más información, consulte Políticas administradas de AWS para AWS Config.	7 de abril de 2022

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • alb-desync-mode-check • autoscaling-capacity-rebala ncing • autoscaling-launchconfig-re quires-imdsv2 • autoscaling-launch-config-h op-límite • autoscaling-multiple-instan ce-types • clb-desync-mode-check • ecs-container-insights-enab led • ecs-fargate-latest-platform- versión • netfw-policy-default-action- paquetes de fragmentos • netfw-policy-default-action- paquetes completos • netfw-policy-rule-group-aso ciado • redshift-audit-logging-enab led • s3- lifecycle-policy-check • waf-regional-rule-not-vacío • waf-regional-rulegroup-not- vacío • waf-regional-webacl-not-vac ío	4 de abril de 2022

- vpc-peering-dns-resolution-comprobar

AWS Config Reglas de política personalizadas	Con esta versión, AWS Config le permite crear reglas de política AWS Config personalizadas utilizando AWS CloudFormation Guard (guard). Guard es un policy-as-code lenguaje que le permite escribir políticas que se apliquen AWS Config sin necesidad de crear funciones Lambda para administrar sus reglas personalizadas. Las reglas escritas con la política de Guard se pueden crear desde la AWS Config consola o mediante la AWS Config regla APIs. Se han actualizado las siguientes páginas de la guía para desarrolladores: • Reglas personalizadas de AWS Config • Creación de reglas AWS Config personalizadas con Guard Se han actualizado los siguientes tipos de datos: • Origen • CustomPolicyDetails • ConfigRuleEvaluationStatus • GetCustomRulePolicy	4 de abril de 2022

	• GetOrganizationCustomRulePolicy • OrganizationCustomPolicyRuleMetadata	
AWS Config admite un nuevo tipo de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en el nuevo tipo de SecurityConfiguration recurso de Amazon EMR. Para obtener más información, consulte Tipos de recursos admitidos.	31 de marzo de 2022
AWS Config actualiza la regla gestionada	En esta versión, AWS Config es compatible con la regla gestionada virtualmachine-resources-protected-by-backup-plan.	29 de marzo de 2022

AWS Config Integración con Amazon CloudWatch Metrics	Con esta versión, AWS Config ahora es compatible con el seguimiento de tus métricas de AWS Config uso y éxito con Amazon CloudWatch en la página del AWS Config panel de control. CloudWatch metrics es un servicio de monitoreo que proporciona datos sobre el rendimiento de sus sistemas, incluida la capacidad de buscar, graficar y generar alarmas a partir de las métricas sobre AWS los recursos. Desde el AWS Config panel de control, puede ver qué tráfico está impulsando su AWS Config uso y las métricas clave para detectar los errores que se han producido en su flujo de trabajo. Se ha actualizado la siguiente página: • Visualización del panel AWS Config	29 de marzo de 2022

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en el nuevo tipo de recurso de Amazon GuardDuty Detector. Para obtener más información, consulte Tipos de recursos admitidos.	24 de marzo de 2022

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • clb-multiple-az • cloudfront-no-deprecated-ssl-protocolos • cloudfront-traffic-to-origin-encriptado • cloudwatch-alarm-action-enabled-comprobar • ec2- no-amazon-key-pair • ec2- paravirtual-instance-check • ec2- token-hop-limit-check • ec2- -attach-deshabilitado transit-gateway-auto-vpc • ecr-private-lifecycle-policy-configurado • efs-access-point-enforce-directorio raíz • efs-access-point-enforce-identidad de usuario • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-comprobar • s3- event-notifications-enabled • sns-topic-message-delivery-habilitado para notificaciones	23 de marzo de 2022

- waf-global-rulegroup-not-vacío
- waf-global-rule-not-vacío

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config actualiza los siguientes paquetes de conformidad: • Mejores prácticas operativas para CIS Critical Security Controls, versión 8 IG1 • Mejores prácticas operativas para los controles de seguridad críticos del CIS, versión 8 IG2 • Mejores prácticas operativas para los controles de seguridad críticos del CIS, versión 8 IG3 • Mejores prácticas operativas para el pilar de seguridad de AWS Well-Architected Framework • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Bajo • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Medio • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Alto • Prácticas operativas recomendadas para MAS Notice 655	16 de marzo de 2022

	• Prácticas operativas recomendadas para NIST 1800-25	
Actualización de seguridad de IAM	Ahora, la política de `AWSConfigServiceRolePolicy` y la política de `AWS_ConfigRole` otorgan permisos adicionales a AWS CloudFormation. Para más información, consulte Políticas administradas de AWS para AWS Config.	14 de marzo de 2022
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config actualiza las siguientes reglas administradas: • aurora-resources-protected-by-plan de respaldo • dynamodb-resources-protected-by-plan de respaldo • ebs-resources-protected-by-plan de respaldo • ec2- -plan resources-protected-by-backup • efs-resources-protected-by-plan de respaldo • fsx-resources-protected-by-plan de respaldo • rds-resources-protected-by-plan de respaldo	10 de marzo de 2022

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos públicos de Amazon Elastic Container Registry. Para obtener más información, consulte Tipos de recursos admitidos.	4 de marzo de 2022
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los nuevos tipos de recursos de Amazon Elastic Compute Cloud. Para obtener más información, consulte Tipos de recursos admitidos.	28 de febrero de 2022
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • codedeploy-auto-rollback-monitor-habilitado • código deploy-ec2-minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-des activado	25 de febrero de 2022

Registro y supervisión en la actualización AWS Config	Con esta versión, se AWS Config actualiza la página Monitoring AWS Config with Amazon EventBridge Events para reemplazar las referencias a Amazon CloudWatch Events. Amazon EventBridge es la forma preferida de gestionar tus eventos. CloudWatch Events y EventBridge son el mismo servicio y API subyacentes, pero EventBridge ofrecen más funciones. Los cambios que realices en CloudWatch cualquiera de las dos consolas EventBridge aparecerán en cada consola. Para obtener más información, consulte Amazon EventBridge.	24 de febrero de 2022
AWS Página de SDK para AWS Config	En esta versión, se AWS Config presenta una página AWS Config sobre cómo usar un AWS SDK. AWS Los kits de desarrollo de software (SDKs) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.	24 de febrero de 2022

Actualización de la política de confianza de los roles de IAM de seguridad	Con esta versión, se AWS Config actualiza la declaración de política de confianza de IAM para incluir protecciones de seguridad en la política de confianza que restringen el acceso a la operación AWS Security Token Service (AWS STS). `sourceARN` and/or `sourceAccountId` Esto ayuda a garantizar que la política de confianza del rol de IAM acceda a sus recursos solo en nombre de los usuarios y los supuestos esperados. Se ha actualizado la siguiente página: • Adición de una política de confianza de IAM a su rol	18 de febrero de 2022

Cambios en el registro de tipos de recursos globales	AWS Config ahora cambia la forma en que se graban los nuevos tipos de recursos globales en AWS Config Recording. Los tipos de recursos globales son AWS recursos que no requieren que especifique una región en el momento de la creación. Antes de este cambio, podía habilitar el registro de los tipos de recursos globales en todas las regiones compatibl es en AWS Config. Tras este cambio, los nuevos tipos de recursos globales incorporados a la AWS Config grabación solo se pueden grabar en la región de origen del servicio en el caso de la partición comercial y AWS GovCloud (EE. UU. y oeste) en el caso de la partición. AWS GovCloud (US) Ahora podrá ver los elementos de configuración de estos nuevos tipos de recursos globales solo en su región de origen y AWS GovCloud (EE. UU. al oeste). Para obtener una lista de las regiones de origen de los tipos de recursos globales incorpora dos después de febrero de 2022, consulta la tabla de la página Registro de todos los tipos de recursos compatibles.	18 de febrero de 2022

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permiso para obtener detalles sobre los entornos de Elastic Beanstalk y una descripción de los ajustes del conjunto de configuraciones de Elastic Beanstalk especificado, obtener un mapa o las versiones de Elasticsearch, describir los grupos de opciones OpenSearch de Amazon RDS disponibles para una base de datos y obtener información sobre una configuración de implementación. CodeDeploy Esta política ahora también otorga permiso para recuperar el contacto alternativo especificado adjunto a una Cuenta de AWS, recuperar información sobre una AWS Organizations política, recuperar una política de repositorio de Amazon ECR, recuperar información sobre una AWS Config regla archivada, recuperar una lista de familias de definiciones de tareas de Amazon ECS, enumerar las unidades organizativas raíz o principal (OUs) de la OU o cuenta secundaria especificada y	10 de febrero de 2022

enumerar las políticas que se adjuntan a la raíz, unidad organizativa o cuenta de destino especificada. Para más información, consulte Políticas administradas de AWS para AWS Config.

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-comprobar • codebuild-project-logging-enabled • codebuild-project-s3 registros cifrados • ec2- -eni-periodic security-group-attached-to • ecr-private-image-scanning-habilitado • ecr-private-tag-immutability-habilitado • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-límite estricto • ecs-task-definition-nonroot-usuario • ecs-task-definition-pid-mode-check • eks-cluster-oldest-supported-versión	10 de febrero de 2022

	• eks-cluster-supported-version • lambda-vpc-multi-az-comprobar • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-no está vacío • rds-cluster-default-admin-comprobar • rds-db-security-group-no permitido • rds-instance-default-admin-comprobar • redshift-default-admin-check • s3- bucket-acl-prohibited • s3- version-lifecycle-policy-check • waf-global-webacl-not-vacío	
Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permiso para crear grupos de CloudWatch registros y transmisiones de Amazon y para escribir registros en las transmisiones de registros creadas. Para más información, consulte Políticas administradas de AWS para AWS Config.	2 de febrero de 2022

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • opensearch-access-control-enabled • opensearch-audit-logging-en abled • opensearch-data-node-fault-tolerancia • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-comprobación de cifrado	31 de enero de 2022
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los tipos de AWS CodeDeploy recursos. Para obtener más informaci ón, consulte Tipos de recursos admitidos.	5 de enero de 2022

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon SageMaker AI. Para obtener más información, consulte Tipos de recursos admitidos.	20 de diciembre de 2021
AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Guía de mejores prácticas operativas para la ciberseguridad de la ENISA para SMEs	20 de diciembre de 2021
AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para NIST 800 172 • Prácticas operativas recomendadas para NIST 800 181 Se ha actualizado el siguiente paquete de conformidad: • Prácticas operativas recomendadas para K-ISMS	18 de noviembre de 2021

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para Amazon API Gateway • Mejores prácticas operativas para AWS Backup • Prácticas operativas recomendadas para CISA Cyber Essentials • Mejores prácticas operativas para DevOps • Prácticas operativas recomendadas para el NIST Privacy Framework v1.0 Se han actualizado los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para el FedRAMP (bajo) • Prácticas operativas recomendadas para FedRAMP (moderadas)	29 de octubre de 2021

AWS Config admite nuevos tipos de recursos	Con esta versión, puedes utilizarla AWS Config para registrar los cambios de configuración de los nuevos tipos de recursos de Amazon OpenSearch Service. Para obtener más información, consulte Tipos de recursos admitidos.	12 de octubre de 2021
AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config actualiza el siguiente paquete de conformidad: • Prácticas operativas recomendadas para MAS TRMG	12 de octubre de 2021

AWS Config es compatible con los nuevos paquetes de conformidad	Con esta versión, AWS Config actualiza los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para cargas de trabajo de material de ABS CCIG 2.0 • Prácticas operativas recomendadas para cargas de trabajo estándar de ABS CCIG 2.0 • Prácticas operativas recomendadas para ACSC Essential 8 • Prácticas operativas recomendadas para ACSC ISM • Mejores prácticas operativas para BNM T RMi • Prácticas operativas recomendadas para la CMMC de nivel 1 • Prácticas operativas recomendadas para la CMMC de nivel 2 • Prácticas operativas recomendadas para la CMMC de nivel 3 • Prácticas operativas recomendadas para la CMMC de nivel 4 • Prácticas operativas recomendadas para la CMMC de nivel 5	30 de septiembre de 2021

- Prácticas operativas recomendadas para la FDA Título 21 CFR Parte 11
- Prácticas operativas recomendadas para FFIEC
- Prácticas operativas recomendadas para MAS Notice 655
- Prácticas operativas recomendadas para NBC TRMG
- Prácticas operativas recomendadas para NERC CIP
- Prácticas operativas recomendadas para el NIST 800-53 rev 5

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permiso para obtener detalles sobre un Amazon OpenSearch Service (OpenSearch Servicio) domain/domains y obtener una lista de parámetros detallada para un grupo de parámetros de base de datos concreto de Amazon Relational Database Service (Amazon RDS). Esta política también otorga permiso para obtener detalles sobre las ElastiCache instantáneas de Amazon. Para más información, consulte Políticas administradas de AWS para AWS Config.	8 de septiembre de 2021
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los nuevos tipos de recursos de Amazon Elastic Compute Cloud. Para obtener más información, consulte Tipos de recursos admitidos.	7 de septiembre de 2021

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config actualiza los siguientes paquetes de conformidad: • Prácticas operativas recomendadas para APRA CPG 234 • Mejores prácticas operativas para CIS AWS Foundations Benchmark v1.4, nivel 1 • Benchmark v1.4, nivel 2, de mejores prácticas operativas para AWS las fundaciones de la CEI • Prácticas operativas recomendadas para los NCSC Cloud Security Principles • Prácticas operativas recomendadas para el NCSC Cyber Assesment Framework • Prácticas operativas recomendadas para NIST 800 171 • Prácticas operativas recomendadas para el NIST CSF • Mejores prácticas operativas para el marco de ciberseguridad del RBI para UCBs • Prácticas operativas recomendadas para RBI MD-ITF	30 de agosto de 2021

- Prácticas operativas recomendadas para NYDFS 23
- Prácticas operativas recomendadas para el PCI DSS 3.2.1

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • aurora-resources-protected-by-plan de respaldo • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-eliminación-deshabilitada • backup-recovery-point-minimum-control de retención • dynamodb-resources-protected-by-plan de respaldo • ebs-resources-protected-by-plan de respaldo • ec2- -plan resources-protected-by-backup • efs-resources-protected-by-plan de respaldo • fsx-resources-protected-by-plan de respaldo • rds-resources-protected-by-plan de respaldo	20 de agosto de 2021

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con el siguiente paquete de conformidad: • Prácticas operativas recomendadas para el NZISM	20 de agosto de 2021
Actualización de la política de seguridad de Amazon SNS	Con esta versión, se AWS Config actualiza la declaración de política de IAM para el tema Amazon SNS cuando se utilizan funciones vinculadas a servicios para incluir protecciones de seguridad que restringen el acceso `sourceARN` and/or `sourceAccountId` en la política temática. Esto ayuda a garantizar que Amazon SNS acceda a sus recursos solo en nombre de los usuarios y los supuestos esperados. Se ha actualizado la siguiente página: • Permisos para el tema de Amazon SNS	17 de agosto de 2021

Actualización de la política de seguridad AWS Lambda	Con esta versión, se AWS Config actualiza la política AWS Lambda basada en recursos para las reglas AWS Config personalizadas a fin de incluir protecciones de seguridad que restrinjan el acceso `sourceARN` and/or `sourceAccountId` en la solicitud de invocación. Esto ayuda a garantizar AWS Lambda el acceso a los recursos únicamente en nombre de los usuarios y escenarios esperados. Se actualizan las siguientes páginas: • AWS::Config::ConfigRule • Desarrollar una regla personalizada para AWS Config	12 de agosto de 2021
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los tipos de recursos de Amazon Kinesis. Para obtener más información, consulte Tipos de recursos admitidos.	6 de agosto de 2021

AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con el siguiente paquete de conformidad: • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Alto Se han actualizado los siguientes paquetes de conformidad: • Mejores prácticas operativas para el pilar de AWS confiabilidad de un marco bien diseñado • Mejores prácticas operativas para el pilar de seguridad de AWS Well-Architected Framework • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Bajo • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Medio • Prácticas operativas recomendadas para la seguridad de HIPAA	30 de julio de 2021

Ejemplos de AWS Lambda funciones para reglas personalizadas AWS Config	En esta versión, se AWS Config proporcionan funciones de ejemplo de Python en Example AWS Lambda Functions for AWS Config Rules (Python).	29 de julio de 2021

Actualización de seguridad de IAM	Ahora, la política de `AWSConfigServiceRolePolicy` y la política de `AWS_ConfigRole` otorgan permisos adicionales para enumerar las etiquetas de un grupo de registro, enumerar las etiquetas de una máquina de estado y enumerar todas las máquinas de estado. Estas políticas ahora otorgan permiso para obtener información sobre una máquina de estado. Estas políticas ahora también admiten permisos adicionales para Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon, Amazon Data Firehose FSx, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon AI, Amazon Simple Notification Service, SageMaker y. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway Para más información, consulte Políticas administradas de AWS para AWS Config.	28 de julio de 2021

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los tipos de AWS Backup recursos. Para obtener más información, consulte Tipos de recursos admitidos.	14 de julio de 2021
AWS Config admite nuevos paquetes de conformidad	Con esta versión, AWS Config es compatible con los siguientes paquetes de conformidad: • Mejores prácticas operativas para los controles de seguridad críticos de CIS, versión 8 IG1 • Mejores prácticas operativas para los controles de seguridad críticos del CIS, versión 8 IG2 • Mejores prácticas operativas para los controles de seguridad críticos del CIS, versión 8 IG3 • Prácticas operativas recomendadas para NIST 1800 25	9 de julio de 2021

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • ssm-document-not-public • s3- account-level-public-access -bloques-periodicos	25 de junio de 2021
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • ec2- instance-multiple-eni-check • elbv2- acm-certificate-required • autoscaling-launch-config-public-ip deshabilitado	10 de junio de 2021

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permiso para ver los permisos de los AWS Systems Manager documentos y la información sobre IAM Access Analyzer. Estas políticas ahora admiten tipos de AWS recursos adicionales para Amazon Kinesis, Amazon, ElastiCache Amazon EMR, Amazon Route 53 y AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Estos cambios de permisos permiten AWS Config invocar el código de solo lectura necesario para admitir estos tipos de recursos APIs . Estas políticas ahora también admiten el filtrado de funciones de Lambda @Edge para la regla lambda-inside-vpc AWS Config administrada. Para más información, consulte Políticas administradas de AWS para AWS Config.	8 de junio de 2021

AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • elasticsearch-logs-to-cloud watch • rds-cluster-multi-az-habili tado • api-gw-associated-with-guer ra • iam-policy-no-statements-wi th-full-access	19 de mayo de 2021
AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los tipos de recursos de Amazon Elastic File System. Para obtener más información, consulte Tipos de recursos admitidos.	13 de mayo de 2021

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permisos que permiten AWS Config realizar llamadas GET de solo lectura a API Gateway para admitir una regla de configuración para API Gateway. Estas políticas también añaden permisos que permiten AWS Config invocar Amazon Simple Storage Service (Amazon S3) en modo de APIs solo lectura, que son necesarios para admitir el nuevo tipo de recurso. `AWS::S3::AccessPoint` Para más información, consulte Políticas administradas de AWS para AWS Config.	10 de mayo de 2021
AWS Config Reglas personalizadas	Se han actualizado las siguientes páginas de la guía para desarrolladores: • Introducción a las reglas personalizadas para AWS Config • Desarrollo de una regla personalizada para AWS Config	30 de abril de 2021

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • aurora-mysql-backtracking-enabled • ec2- instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-habilitado para la actualización • redshift-enhanced-vpc-routing-habilitado	15 de abril de 2021

Actualización de seguridad de IAM	La `AWSConfigServiceRolePolicy` política y la `AWS_ConfigRole` política ahora otorgan permiso para ver información sobre documentos AWS Systems Manager específicos. Estas políticas ahora también admiten tipos de AWS recursos adicionales para AWS Backup Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis, Amazon AI y Amazon Route SageMaker 53. AWS Database Migration Service Estos cambios de permisos permiten AWS Config invocar el código de solo lectura APIs necesario para admitir estos tipos de recursos. Para más información, consulte Políticas administradas de AWS para AWS Config.	14 de abril de 2021

El cumplimiento del paquete de conformidad como elementos de configuración () CIs	Con esta versión, AWS Config admite el cumplimiento de los paquetes de conformidad como elementos de configura ción. Esto le permite: • Ver una escala de tiempo de los cambios en el estado de conformidad de sus paquetes de conformidad • Agregar el cumplimiento de los paquetes de conformid ad en varias cuentas y regiones • Utilizar consultas avanzadas para comprobar el cumplimiento de sus paquetes de conformidad Se han actualizado los siguientes tipos de datos: • DescribeAggregateC omplianceByConform ancePacks • GetAggregateConfor mancePackComplianc eSummary Se han actualizado las siguientes páginas de la guía para desarrolladores: • Visualización de los datos de conformidad en el panel de paquetes de conformidad	30 de marzo de 2021

	• Visualización de la línea de tiempo del historial de conformidad de los paquetes de conformidad • Visualización de los datos de conformidad en el panel del agregador • Consulta del estado de la configuración actual de los recursos AWS • Tipos de recursos admitidos	
Actualización de la paginación	Con esta versión, la función de consultas AWS Config avanzadas ahora admite la paginación de las consultas que contienen funciones de agregación, como COUNT y SUM. Ahora puede utilizar las consultas avanzadas para obtener resultados completos para las consultas agregadas mediante la paginación, que antes estaba limitada a 500 filas. Para obtener más información, consulte Consulta el estado de la configuración actual de los recursos AWS	26 de marzo de 2021
Compatibilidad de regiones	Con esta versión, AWS Config and AWS Config Rules ahora es compatible con la región de Asia Pacífico (Osaka).	4 de marzo de 2021

AWS Config admite nuevos tipos de recursos	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los tipos de recursos de Amazon Elastic Container Registry, Amazon Elastic Container Service y Amazon Elastic Kubernetes Service. Para obtener más información, consulte Tipos de recursos admitidos.	25 de febrero de 2021
Compatibilidad con el cifrado KMS	Con esta versión, AWS Config le permite utilizar el cifrado basado en KMS en los objetos entregados mediante entrega en cubos AWS Config de S3. Se han actualizado los siguientes tipos de datos: • DeliveryChannel • PutDeliveryChannel Se han actualizado las siguientes páginas de la guía para desarrolladores: • Permisos para la clave de KMS • Permisos para el rol de IAM asignado a AWS Config	16 de febrero de 2021

AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administr adas: • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	16 de febrero de 2021
Compatibilidad de las consultas guardadas en nuevas regiones	Con esta versión, las consultas guardadas ahora se admiten en las regiones AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste).	15 de febrero de 2021
Compatibilidad de la agregació n de datos de varias cuentas y regiones en nuevas regiones	Con esta versión, la agrupació n de datos de varias cuentas y regiones ahora es compatibl e en las regiones de África (Ciudad del Cabo) y Europa (Milán). Para obtener más información, consulte Acumulación de datos de varias cuentas y regiones.	15 de febrero de 2021
Compatibilidad de las consultas avanzadas con nuevas regiones	Con esta versión, ahora se admiten las consultas avanzadas en las regiones de África (Ciudad del Cabo) y Europa (Milán). Para obtener más información, consulte Consulta el estado de la configuración actual de los recursos. AWS	15 de febrero de 2021

AWS Config notificación del historial de documentación disponible a través de una fuente RSS	Ahora puede recibir notificaciones sobre las actualizaciones de la AWS Config documentación suscribiéndose a una fuente RSS.	1 de enero de 2021

Actualizaciones anteriores

En la siguiente tabla se describe el historial de publicación de la documentación AWS Config anterior al 31 de diciembre de 2020.

Cambio	Description (Descripción)	Fecha de lanzamiento
Compatibilidad con las consultas guardadas	Con esta versión, AWS Config le permite guardar sus consultas. Tras guardar la consulta, puede buscarla, copiarla en el editor de consultas, editarla o eliminarla. Para obtener más información sobre cómo guardar una consulta, consulte Consulta mediante el editor de consultas SQL para AWS Config (consola) y Consulta mediante el editor de consultas SQL para AWS Config (AWS CLI). Para obtener más información al respecto APIs, consulte la referencia AWS Config de la API: • PutStoredQuery • GetStoredQuery • ListStoredQueries • DeleteStoredQuery	21 de diciembre de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
	Consulte también Límites de los servicios para AWS Config.	
Compatibilidad con las comprobaciones de procesos	Con esta versión, AWS Config admite las comprobaciones de procesos, es decir, un tipo de AWS Config regla que le permite realizar un seguimiento de las tareas externas e internas que requieren verificación como parte de los paquetes de conformidad. Las comprobaciones de procesos permiten enumerar el cumplimiento de los requisitos y las acciones en una única ubicación. Para obtener más información sobre las comprobaciones de procesos, consulte el AWS Config Comprobaciones de procesos dentro de un paquete de conformidad para AWS Config tema y la PutExternalEvaluationAPI.	17 de diciembre de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administradas: • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-habilitado • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-habilitado • rds-cluster-iam-authentication-habilitado • redshift-cluster-kms-enabled • s3- -prohibido bucket-level-public-access • subnet-auto-assign-public-ip desactivado • vpc-network-acl-unused-comprobar	17 de diciembre de 2020
AWS Config apoya AWS Network Firewall	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en sus AWS Network Firewall FirewallPolicy tipos de recursos y en los de Firewall. RuleGroup Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	4 de diciembre de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
Actualización de la documentación	AWS Config se agregó soporte para la agregación de datos de recursos de toda la organización en una cuenta de administrador delegado. Ahora puede utilizar una cuenta de administrador delegada para agregar la configuración de recursos y los datos de conformidad de todas las cuentas de miembros de una en AWS Organizations. Para obtener más información, consulte PutConfigurationAggregator, Creación de agregadores para AWS Config y Registro de un administrador delegado para AWS Config.	4 de diciembre de 2020
AWS Config admite nuevos paquetes de conformidad	• Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Bajo • Prácticas operativas recomendadas para el Esquema Nacional de Seguridad (ENS) Medio • Prácticas operativas recomendadas para el NCSC Cyber Assesment Framework • Mejores prácticas operativas para el marco de ciberseguridad del RBI para UCBs	30 de octubre de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevos paquetes de conformidad	• Prácticas operativas recomendadas para ACSC Essential 8 • Prácticas operativas recomendadas para ACSC ISM: parte 1 • Prácticas operativas recomendadas para IA y ML • Prácticas operativas recomendadas para la gestión de activos • Prácticas operativas recomendadas para BCP y DR • Prácticas operativas recomendadas para EC2 • Prácticas operativas recomendadas para K-ISMS • Prácticas operativas recomendadas para el equilibrado de carga • Prácticas operativas recomendadas para el registro • Prácticas operativas recomendadas para el monitoreo • Prácticas operativas recomendadas para soluciones sin servidor	22 de octubre de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevos paquetes de conformidad	• Prácticas operativas recomendadas para APRA CPG 234 • Prácticas operativas recomendadas para el FedRAMP (bajo) • Prácticas operativas recomendadas para MAS Notice 655 • Prácticas operativas recomendadas para NBC TRMG • Prácticas operativas recomendadas para los NCSC Cloud Security Principles • Prácticas operativas recomendadas para RBI MD-ITF	15 de octubre de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevos paquetes de conformidad	• Prácticas operativas recomendadas para cargas de trabajo de material de ABS CCIG 2.0 • Prácticas operativas recomendadas para cargas de trabajo estándar de ABS CCIG 2.0 • Mejores prácticas operativas para BNM T RMi • Prácticas operativas recomendadas para la resiliencia de datos • Prácticas operativas recomendadas para lagos de datos y servicios de análisis • Prácticas operativas recomendadas para el cifrado y la administración de claves • Prácticas operativas recomendadas para la FDA Título 21 CFR Parte 11 • Prácticas operativas recomendadas para recursos de acceso público • Prácticas operativas recomendadas para MAS TRMG • Prácticas operativas recomendadas para NERC CIP BCSI • Prácticas operativas recomendadas para NYDFS 23	8 de octubre de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevos paquetes de conformidad	• Mejores prácticas operativas para el pilar de confiabilidad de AWS un marco de trabajo bien diseñado • Mejores prácticas operativas para el pilar de seguridad de AWS Well-Architected Framework • Prácticas operativas recomendadas para servicios de computación • Prácticas operativas recomendadas para servicios de bases de datos • Prácticas operativas recomendadas para servicios de administración y gobernanza • Prácticas operativas recomendadas para redes y servicios de entrega de contenido • Prácticas operativas recomendadas para los servicios de seguridad, identidad y conformidad • Prácticas operativas recomendadas para servicios de almacenamiento	26 de octubre de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevos paquetes de conformidad	• Prácticas operativas recomendadas para FedRAMP (moderadas) • Prácticas operativas recomendadas para FFIEC • Prácticas operativas recomendadas para la seguridad de la HIPAA • Prácticas operativas recomendadas para el NIST 800-53 rev 4 • Prácticas operativas recomendadas para NIST 800 171	28 de septiembre de 2020
Actualización de la documentación	Se han actualizado los siguientes temas de paquetes de conformidad. • Requisito previo para los paquetes de conformidad para AWS Config • Implementación de paquetes de conformidad para AWS Config • Gestión de paquetes de conformidad para AWS Config todas las cuentas de su organización	28 de septiembre de 2020
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administradas: • iam-customer-policy-blocked-kms-acciones • iam-inline-policy-blocked-kms-acciones	17 de septiembre de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite la AWS WAF versión 2	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en su WebACL, IPSet RegexPatt ernSet RuleGroup, y los tipos de ManagedRuleSet recursos de la AWS WAF versión 2. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	1 de septiembre de 2020
Actualización de la documenta ción	Se ha añadido una nota en Acceso completo a AWS Config sobre la creación de permisos personalizados que concedan acceso total. Se ha actualizado la documentación de las siguientes reglas: • habilitado para bucket-server-side-encryption s3 • ec-2 instance-detailed-monitoring-enabled • ec-2 managedinstance-platform-check	24 de agosto de 2020
Actualización de la documenta ción	Se han actualizado las plantillas de Prácticas operativas recomendadas para el PCI DSS 3.2.1 y Prácticas operativas recomendadas para el NIST CSF.	14 de agosto de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
Actualización de la documentación	Se han agregado las consultas de relaciones de ejemplo. Para obtener más información, consulte Ejemplos de consultas de relación para AWS Config.	30 de julio de 2020
Actualización de la documentación	Se han actualizado los siguientes tipos de datos: • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus	23 de julio de 2020
AWS Config admite el tipo de recurso AWS Systems Manager	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en el tipo de recurso de datos del archivo AWS Systems Manager. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	9 de julio de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
Actualización de la documentación	Se han actualizado las plantillas de Prácticas operativas recomendadas para AWS Identity and Access Management y Prácticas operativas recomendadas para el PCI DSS 3.2.1.	9 de julio de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config actualiza las reglas administradas	Con esta versión, AWS Config es compatible con las siguientes reglas administradas: • account-part-of-organizations • alb-http-drop-invalid-habilitado para encabezado • alb-waf-enabled • cloudfront-default-root-object-configurado • cloudfront-origin-access-identity-habilitado • cloudfront-origin-failover-enabled • cloudfront-sni-enabled • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-comprobar • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-acceso • eks-secrets-encrypted • elasticsearch-node-to-node-comprobación de cifrado • elb-cross-zone-load-habilitado para el equilibrio • elb-tls-https-listeners-solo • iam-no-inline-policy-comprobar	9 de julio de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
	• rds-cluster-deletion-protection-habilitado • rds-in-backup-plan • rds-instance-deletion-protection-habilitado • rds-instance-iam-authentication-habilitado • rds-logging-enabled • redshift-backup-enabled • waf-classic-logging-enabled • wafv2-logging-enabled Para obtener más información, consulte Lista de reglas AWS Config administradas.	
Compatibilidad de la agregación de datos de varias cuentas y regiones en nuevas regiones	Con esta versión, ahora admite la agregación de datos de varias cuentas y regiones en las regiones de Asia-Pacífico (Hong Kong) y Medio Oriente (Baréin). Para obtener más información, consulte Multi-Account Multi-Region Data Aggregation y Solución de problemas de agregación de datos multicuenta y multirregión para AWS Config.	1 de julio de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
Compatibilidad de las consultas avanzadas con nuevas regiones	Con esta versión, las consultas avanzadas ahora son compatibl es con las regiones de Asia-Pací fico (Hong Kong) y Medio Oriente (Baréin). Para obtener más informaci ón, consulte Consulta del estado de la configuración actual de AWS los recursos con AWS Config.	1 de julio de 2020
Actualización de la documenta ción	Se ha actualizado la documentación de las siguientes reglas: • ec2- -comprobar managedin stance-association-compliance-status • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • rds-snapshots-public-prohibited • s3- bucket-policy-grantee-check	30 de junio de 2020
Actualización de la documenta ción	La documentación se ha actualizado con información sobre la seguridad de AWS Config. Consulte Seguridad en AWS Config.	24 de junio de 2020
Actualización de la documenta ción	AWS Control Tower Se ha actualiza do la plantilla del paquete de conformidad de Detective Guardrail s. Para obtener más información, consulte AWS Paquete de conformid ad con las barandillas Control Tower Detective.	4 de junio de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite un nuevo paquete de conformidad	Con esta versión, AWS Config es compatible con el paquete de conformidad CSF con las mejores prácticas operativas para el NIST. Para obtener más información, consulte Prácticas operativas recomendadas para el NIST CSF.	29 mayo de 2020
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administradas: • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec-2 ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s3- bucket-default-lock-enabled • s3- default-encryption-kms • securityhub-enabled • sns-encrypted-kms Para obtener más información, consulte Lista de reglas AWS Config administradas.	28 de mayo de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
Compatibilidad con el administrador delegado	Con esta versión, puede implementar AWS Config reglas y paquetes de conformidad desde cualquier cuenta de miembro delegado de su organización, además de la cuenta de administración. Para obtener más información al respecto APIs, consulte la referencia de la AWS Config API: • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus Para obtener más información, consulte Límites de los servicios para AWS Config.	27 de mayo de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config reglas: Soporte regional	Con esta versión, se admiten pocas AWS Config reglas en las regiones de África (Ciudad del Cabo) y Europa (Milán). Para obtener una lista detallada de las reglas y las regiones en las que se admiten, consulte Lista de reglas AWS Config administradas.	28 de abril de 2020
AWS Config es compatible con los nuevos paquetes de conformidad	Con esta versión, AWS Config admite dos paquetes de conformid ad. • AWS Paquete de conformidad con las barandillas Control Tower Detective • Prácticas operativas recomenda das para CIS Para obtener más información, consulte Plantillas de ejemplo de paquete de conformidad para AWS Config.	22 de abril de 2020
AWS Config es compatible con AWS Secrets Manager	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración de su secreto de Secrets Manager. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	20 de abril de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administradas: • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-comprobar Para obtener más información, consulte Lista de reglas AWS Config administradas.	16 de abril de 2020
Compatibilidad del paquete de conformidad en nuevas regiones	Con esta versión, ahora se admiten los paquetes de conformidad con las regiones de Asia-Pacífico (Hong Kong) y Medio Oriente (Baréin). Para obtener más información, consulte Conformance Packs.	8 de abril de 2020
Actualización de la documentación	AWS Config los límites están disponibles en esta guía para desarrolladores. Para obtener más información, consulte Límites de los servicios para AWS Config.	8 de abril de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
Actualización de la documentación	Los recursos de terceros que se administran (es decir,created/updated/deleted) mediante CloudFormation el registro se registran automáticamente AWS Config como elementos de configuración. Para obtener más información, consulte Grabación de configuraciones con AWS Config recursos de terceros mediante AWS CLI.	30 de marzo de 2020
Actualización de la documentación	Las reglas AWS Config administradas se actualizan para incluir Región de AWS información. Para obtener más información, consulte Lista de reglas AWS Config administradas.	27 de marzo de 2020
AWS Config admite el tipo de recurso Amazon SNS	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en su tema de Amazon SNS. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	6 de marzo de 2020
Compatibilidad de la agregación de datos de varias cuentas y regiones en nuevas regiones	Con esta versión, la agrupación de datos de varias cuentas y regiones se admite ahora en la región de Europa (Estocolmo). Para obtener más información, consulte Multi-Account Multi-Region Data Aggregation.	5 de marzo de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
Compatibilidad de las consultas avanzadas con nuevas regiones	Con esta versión, las consultas avanzadas se admiten ahora en la región de Europa (Estocolmo). Para obtener más información, consulte Consulta del estado de la configuración actual de AWS los recursos con AWS Config.	5 de marzo de 2020
AWS Config le permite ejecutar consultas avanzadas con agregadores de configuración	Con esta versión, se AWS Config añade la posibilidad de ejecutar consultas avanzadas basadas en las propiedades de configuración de los recursos con agregadores de configuración, lo que permite ejecutar las mismas consultas en varias cuentas y regiones. Para obtener más información, consulte Consulta del estado de la configuración actual de AWS los recursos con AWS Config. Con esta versión, AWS Config añade la `SelectAggregateResourceConfig` API. Para obtener más información, consulta SelectAggregateResourceConfigla referencia de la AWS Config API:	28 de febrero de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite el tipo de recurso Amazon SQS	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en su cola de Amazon SQS. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	13 de febrero de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS CloudFormation soporte para paquetes de conformidad	Con esta versión, se agregó AWS CloudFormation soporte para los siguientes recursos: `AWS::Config::ConformancePack` `yOrganizationConformancePack` . • AWS::Config::ConformancePack Utilice el `AWS::Config::ConformancePack` recurso para crear un paquete de conformidad que sea un conjunto de AWS Config reglas que se puedan implementar fácilmente en una cuenta, una región y en toda la AWS organización. • AWS::Config::OrganizationConformanceEmpaque Utilice el `AWS::Config::OrganizationConformancePack` recurso para crear un paquete de conformidad organizacional que contenga información sobre paquetes de conformidad que se AWS Config crean en las cuentas de los miembros.	13 de febrero de 2020

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administradas: • api-gw-execution-logging-habilitado • ec2-stopped-instance • elasticache-redis-cluster-automatic-verificación de respaldo • emr-master-no-public-IP • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • bloques s3 account-level-public-access - • sagemaker-endpoint-configuration-kms-configurado por clave • service-vpc-endpoint-enabled Para obtener más información, consulte Lista de reglas AWS Config administradas.	20 de diciembre de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
Registro de configuraciones para los tipos de recursos personalizados	En esta versión, se AWS Config introduce la compatibilidad con las configuraciones de registro para tipos de recursos personalizados. Puede publicar los datos de configuración de recursos de terceros AWS Config y ver y supervisar el inventario de recursos y el historial de configura ción mediante la AWS Config co nsola y APIs. Para obtener más información, consulte Grabación de configuraciones con AWS Config recursos de terceros mediante AWS CLI. Para obtener más información al respecto APIs, consulte la referencia AWS Config de la API: • DeleteResourceConfig • PutResourceConfig	20 de noviembre de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
Paquetes de conformidad	Con esta versión, AWS Config presenta los paquetes de conformidad. Los paquetes de conformidad le permiten empaquetar un conjunto de AWS Config reglas y acciones correctivas que luego se pueden implementar juntas como una sola entidad en toda la organización. AWS Para obtener más información, consulte Conformance Packs. Para obtener más información al respecto APIs, consulte la referencia de la AWS Config API: • DeleteOrganizationConformancePack • DeleteOrganizationConformancePack • DescribeConformancePacks • DescribeConformancePacks • DescribeConformancePackStatus • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetConformancePackComplianceDetails • GetConformancePackComplianceSummary • GetOrganizationConformancePackDetailedStatus, • PutConformancePack	19 de noviembre de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
	• PutOrganizationConformancePack	
AWS Config admite los tipos de AWS Key Management Service recursos y OpenSearch servicios de Amazon	Con esta versión, puedes utilizarla AWS Config para registrar los cambios de configuración en tu dominio y AWS Key Management Service clave de Amazon OpenSearch Service. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	11 de noviembre de 2019
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administradas: • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-solo • kms-cmk-not-scheduled-para su eliminación • sagemaker-notebook-no-direct-acceso a internet • sagemaker-notebook-instance-kms-configurado por clave • shield-drt-access Para obtener más información, consulte Lista de reglas AWS Config administradas.	10 de octubre de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite el tipo de recurso Amazon RDS	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en su Amazon Relational Database Service (Amazon RDS DBCluster) DBCluster y en Snapshot. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	17 de septiembre de 2019
AWS Config admite el tipo de recurso Amazon QLDB	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en el tipo de recurso de registro de Amazon Quantum Ledger Database (QLDB). Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	10 de septiembre de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config le permite aplicar la corrección automática a los recursos no conformes , según lo evaluado por las reglas AWS Config	Con esta versión, se AWS Config introduce el soporte para aplicar la corrección automática mediante documentos de AWS Systems Manager automatización en recursos no conformes, según lo evaluado por AWS Config Rules. Para obtener más información, consulte Corregir los recursos no conformes con AWS Config. Con esta versión, AWS Config agrega las siguientes novedades. APIs Para obtener más información, consulte la Referencia de la API de AWS Config : • PutRemediationExceptions • DescribeRemediationExceptions • DeleteRemediationExceptions	5 de septiembre de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config actualiza las reglas gestionadas	Con esta versión, AWS Config es compatible con las siguientes reglas administradas: • alb-http-to-https-comprobación de redireccionamiento • api-gw-cache-enabled-y encriptado • api-gw-endpoint-type-comprobar • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-comprobar • elb-deletion-protection-enabled • lambda-concurrency-check • lambda-dlq-check • lambda-inside-vpc • shield-advanced-enabled-autorenew • vpc-vpn-2-tunnels-up Para obtener más información, consulte Lista de reglas AWS Config administradas.	22 de agosto de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config actualiza las reglas administr adas	Con esta versión, AWS Config actualiza las siguientes reglas administradas: • cloudfront-viewer-policy-https • ec-2 instance-no-public-ip • ec-2 security-group-attached-to -es • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-comprobar • vpc-sg-open-only-to-authorized-ports Para obtener más información, consulte Lista de reglas AWS Config administradas.	31 de julio de 2019
AWS Config admite los tipos de recursos de Amazon EC2	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en los siguientes recursos de Amazon EC2: VPCEndpoint VPCEndpoint Service y VPCPeering Connection. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	12 de julio de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config le permite gestionar las AWS Config reglas en todos los Cuentas de AWS ámbitos de una organización	Con esta versión, AWS Config introduce la compatibilidad con la gestión de AWS Config reglas Cuentas de AWS en toda la organización. Puede crear, actualizar y eliminar AWS Config reglas de forma centralizada en todas las cuentas de su organización. Para obtener más información, consulte Administración de AWS Config reglas en todas las cuentas de su organización. Para obtener más información al respecto APIs, consulta la referencia AWS Config de la API: • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule	9 de julio de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite los tipos de recursos Amazon S3 y Amazon EC2	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en el AccountPublicAccessBlock recurso de Amazon S3 y en los siguientes recursos de Amazon EC2; NatGateway EgressOnlyInternet Gateway, y. FlowLog Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	17 de mayo de 2019
AWS Config actualiza las reglas administr adas	Con esta versión, AWS Config actualiza las siguientes reglas administradas: • s3- bucket-public-read-prohibited • s3- bucket-public-write-prohibited Para obtener más información, consulte Lista de reglas AWS Config administradas.	7 de mayo de 2019
AWS Config permite eliminar una acción correctiva mediante Consola de administración de AWS.	En esta versión, se AWS Config introduce la posibilidad de eliminar una acción correctiva mediante. Consola de administración de AWS Para obtener más información, consulte Corregir los recursos no conformes con AWS Config.	24 de abril de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevas reglas administradas	Esta versión admite una nueva regla administrada: fms-shield-resource-policy-comprobar. Para obtener más información, consulte Lista de reglas AWS Config administradas.	7 de abril de 2019
AWS Config admite el tipo de recurso Amazon API Gateway	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los siguientes recursos de Amazon API Gateway: WebSocket Api (API), RestApi (API REST), Stage (etapa WebSocket API) y Stage (etapa REST API). Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	20 de marzo de 2019
AWS Config le permite ejecutar consultas avanzadas	Con esta versión, AWS Config añade compatibilidad para ejecutar consultas avanzadas en función de las propiedades de configuración de los recursos. Para obtener más información, consulte Consulta del estado de la configuración actual de AWS los recursos con AWS Config. Con esta versión, AWS Config agrega la `SelectResourceConfig` API. Para obtener más información, consulta SelectResourceConfigla referencia de la AWS Config API:	19 de marzo de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config le permite asignar etiquetas a sus AWS Config recursos	Con esta versión, AWS Config introduce la compatibilidad con el control de acceso basado en etiquetas para tres AWS Config recursos: `ConfigRule`, `ConfigurationAggregator`, y`AggregationAuthorization` . Para obtener más información, consulte Etiquetado de los recursos de AWS Config. En esta versión, puede añadir, quitar o crear una lista de las etiquetas de los recursos de AWS Config co n las siguientes tipos de datos. Para obtener más información, consulte la Referencia de la API de AWS Config : • ListTagsForResource • TagResource • UntagResource	14 de marzo de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config permite aplicar medidas correctivas a los recursos no conformes , según lo evaluado por las reglas. AWS Config	En esta versión, se AWS Config introduce la posibilidad de aplicar medidas correctivas mediante documentos de AWS Systems Manager automatización a los recursos no conformes, según lo evaluado por Rules. AWS Config Para obtener más información, consulte Corregir los recursos no conformes con AWS Config. Con esta versión, AWS Config agrega las siguientes novedades. APIs Para obtener más información, consulte la Referencia de la API de AWS Config : • DeleteRemediationConfiguration • DescribeRemediationConfigurations • DescribeRemediationExecutionStatus • PutRemediationConfigurations • StartRemediationExecution	12 de marzo de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config apoya AWS Config las normas de la región de China (Ningxia)	Esta versión solo admite 54 AWS Config reglas en la región de China (Ningxia). Para obtener más información, consulte Lista de reglas AWS Config administradas. Sin embargo, actualmente AWS Config no admite las siguiente s reglas en la región de China (Ningxia): • acm-certificate-expiration-check • cmk-backing-key-rotation-ha bilitado • cloudformation-stack-drift-detection -comprobar • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-habilitado para la validación • codebuild-project-envvar-awscred-comprobar • codebuild-project-source-repo-comprobar la URL • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-e nabled • elb-acm-certificate-required • encrypted-volumes	12 de marzo de 2019

Cambio	Description (Descripción)	Fecha de lanzamiento
	• fms-webacl-resource-policy-comprobar • fms-webacl-rulegroup-association-comprobar • guardduty-enabled-centralized • lambda-function-public-access-prohibido • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-h abilitado para mfa • root-account-mfa-enabled • s3- bucket-blacklisted-actions-prohibited • s3- bucket-policy-grantee-check • s3- bucket-policy-not-more - permisivo • s3- bucket-public-read-prohibited • s3- bucket-public-write-prohibited • habilitado para bucket-server-side-encryption s3 • s3- bucket-ssl-requests-only	

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevas reglas gestionadas	Esta versión admite las nuevas reglas administradas que se indican a continuación: • iam-user-mfa-enabled • s3- bucket-policy-grantee-check Para obtener más información, consulte Lista de reglas AWS Config administradas.	21 de enero de 2019
AWS Config admite el tipo de recurso Service Catalog	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los siguientes recursos de Service Catalog: CloudFromation producto, producto aprovisionado y cartera. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	11 de enero de 2019
Compatibilidad con reglas vinculadas a servicios AWS Config	En esta versión, se AWS Config añade una nueva regla de configuración gestionada que permite a otros AWS servicios crear AWS Config reglas en tu cuenta. Para obtener más información, consulte Roles vinculados a servicios de AWS Config.	20 de noviembre de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config le permite agregar los datos de configuración de AWS los recursos	Con esta versión, AWS Config introduce la compatibilidad con la agregación de los datos de configura ción de los AWS recursos. Para obtener más información, consulte Visualización de los datos de conformidad e inventario en el panel de control del agregador para AWS Config. Con esta versión, AWS Config agrega las siguientes novedades APIs. Para obtener más información, consulte la Referencia de la API de AWS Config : • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceCounts • GetAggregateResourceConfig • ListAggregateDiscoveredResources	19 de noviembre de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevas reglas gestionadas	Esta versión admite las nuevas reglas administradas que se indican a continuación: • cloudformation-stack-drift-detection-comprobar • codepipeline-deployment-count-check • codepipeline-region-fanout-check Para obtener más información, consulte Lista de reglas AWS Config administradas.	19 de noviembre de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevas reglas gestionadas	Esta versión admite las nuevas reglas administradas que se indican a continuación: • access-keys-rotated • cloud-trail-cloud-watch-registros habilitados • cloud-trail-encryption-enabled • cloud-trail-log-file-habilitada para validación • cmk-backing-key-rotation-habilitado • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-comprobar • iam-root-access-key-comprobar • iam-user-unused-credentials-comprobar • mfa-enabled-for-iam-acceso a la consola • multi-region-cloudtrail-enabled • root-account-hardware-mfa-habilitado • vpc-flow-logs-enabled Para obtener más información, consulte Lista de reglas AWS Config administradas.	12 de noviembre de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevas reglas gestionadas	Esta versión admite las nuevas reglas administradas que se indican a continuación: • dynamodb-table-encryption-enabled • elb-logging-enabled • rds-instance-public-access-comprobar • vpc-default-security-group-cerrado Para obtener más información, consulte Lista de reglas AWS Config administradas.	24 de octubre de 2018
Soporte de historial de conformidad	Con esta versión, AWS Config ahora es posible almacenar el historial de conformidad de los recursos según lo evaluado por AWS Config Rules. Para obtener más información, consulte Visualización del cronograma del historial de conformidad para recursos y reglas.	18 de octubre de 2018
La agregación de varias cuentas y regiones ahora se admite en nuevas regiones	Con esta versión, la agrupación de datos de varias cuentas y regiones ahora se admite en seis nuevas regiones. Para obtener más información, consulte Multi-Account Multi-Region Data Aggregation.	4 de octubre de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite permisos a nivel de recurso para AWS Config las acciones de Rules APIs	Con esta versión, AWS Config admite permisos a nivel de recursos para determinadas AWS Config acciones de la API de reglas. Para obtener más información sobre las admitidas APIs, consulte. Permisos a nivel de recursos compatibles para las acciones de la API de AWS Config reglas	1 de octubre de 2018
AWS Config admite el tipo CodePipeline de recurso	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en el tipo de AWS CodePipeline recurso. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	12 de septiembre de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevas reglas administradas	Esta versión admite las nuevas reglas administradas que se indican a continuación: • ec2- -administrador instance-managed-by-systems • ec2- -comprobar managedinstance-association-compliance-status • ec2- -comprobar managedinstance-patch-compliance-status • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s3- bucket-blacklisted-actions-prohibited • s3- bucket-policy-not-more -permisivo Para obtener más información, consulte Lista de reglas AWS Config administradas.	5 de septiembre de 2018
AWS Config admite el tipo de recurso AWS Systems Manager	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los tipos de recursos de cumplimiento de parches y cumplimiento de asociaciones de AWS Systems Manager. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	9 de agosto de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config le permite eliminar sus AWS Config datos mediante Consola de administración de AWS	Con esta versión, AWS Config introduce la compatibilidad con el uso durante el período de retención Consola de administración de AWS. En el Consola de administración de AWS, puede seleccionar un período de retención de datos personalizado para su`ConfigurationItems` . Para obtener más información, consulte Eliminar AWS Config datos.	7 de agosto de 2018
AWS Config admite el tipo AWS Shield de recurso	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en el tipo de recurso de AWS Shield protecció n. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	7 de agosto de 2018
AWS Config admite AWS PrivateLink	Con esta versión AWS PrivateLi nk, AWS Config es compatible y le permite enrutar datos entre su Amazon Virtual Private Cloud (VPC) y AWS Config completamente dentro de la red. AWS Para obtener más información, consulte Uso de AWS Config con los puntos de conexión de interfaz de Amazon VPC.	31 de julio de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config le permite eliminar sus datos AWS Config	Con esta versión, AWS Config introduce la compatibilidad con el período de retención. AWS Config le permite eliminar sus datos especific ando un período de retención para su`ConfigurationItems` . Para obtener más información, consulte Eliminar AWS Config datos. Con esta versión, AWS Config agrega las siguientes novedades APIs. Para obtener más información, consulte la Referencia de la API de AWS Config : • PutRetentionConfiguration • DescribeRetentionConfigurations • DeleteRetentionConfiguration	25 de mayo de 2018
AWS Config admite nuevas reglas gestionad as	Esta versión admite las dos nuevas reglas administradas que se indican a continuación: • lambda-function-settings-check • s3- bucket-replication-enabled • iam-policy-blacklisted-check Para obtener más información, consulte Lista de reglas AWS Config administradas.	10 de mayo de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite el tipo AWS X-Ray de recurso	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en el tipo de AWS X-Ray EncryptionConfig recurso. Para obtener más informaci ón, consulte Tipos de recursos compatibles para AWS Config.	1 de mayo de 2018
AWS Config admite AWS Lambda el tipo de recurso y una nueva regla administrada	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en el tipo de recurso de la AWS Lambda función. Para obtener más informaci ón, consulte Tipos de recursos compatibles para AWS Config. Esta versión también admite la regla administrada lambda-function-pu blic-access-prohibido. Para obtener más información, consulte AWS ConfigReglas de administradas.	25 de abril de 2018
AWS Config admite el tipo AWS Elastic Beanstalk de recurso	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en los recursos de la AWS Elastic Beanstalk aplicación, la versión de la aplicación y el entorno. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	24 de abril de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevas reglas administradas	Esta versión admite las dos nuevas reglas administradas que se indican a continuación: • fms-webacl-resource-policy-comprobar • fms-webacl-rulegroup-association-comprobar Para obtener más información, consulte Lista de reglas AWS Config administradas.	4 de abril de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
Acumulación de datos de multicuentas y multiregiones	Con esta versión, se AWS Config introduce la agregación de datos multicuenta y multirregión. Esta función le permite agregar AWS Config datos de varias cuentas o de una organización y varias regiones en una cuenta agregadora. Para obtener más información, consulte Multi-Account Multi-Region Data Aggregation. Con esta versión, AWS Config añade las siguientes novedades APIs. Para obtener más información, consulte la Referencia de la API de AWS Config : • PutConfigurationAggregator • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAuthorization • DescribeAggregationAuthorizations • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRule • DescribeConfigurationAggregators • DescribeConfigurationAggregatorSourcesStatus • DeleteAggregationAuthorization	4 de abril de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
	• DeleteConfigurationAggregator	
Supervisión AWS Config con Amazon CloudWatch Events	Con esta versión, utilice Amazon CloudWatch Events para detectar los cambios en el estado de los AWS Config eventos y reaccionar ante ellos. Para obtener más información, consulte Monitorización AWS Config con Amazon EventBridge.	29 de marzo de 2018
Nueva operación API	Con esta versión, AWS Config añade compatibilidad con la BatchGetResourceConfigAPI, lo que le permite recuperar por lotes el estado actual de uno o más de sus recursos.	20 de marzo de 2018
AWS Config admite el tipo AWS WAF RuleGroup de recurso	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los recursos RuleGroup regionales del AWS WAF RuleGroup y AWS del WAF. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	15 de febrero de 2018

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config es compatible con las nuevas reglas gestionadas	Esta versión admite las nuevas reglas administradas que se indican a continuación: • elb-acm-certificate-required • elb-custom-security-policy-comprobación de SSL • elb-predefined-security-policy-comprobación de SSL • codebuild-project-envvar-awscred-comprobar • codebuild-project-source-repo-comprobación de URL • iam-group-has-users-comprobar • habilitado para bucket-server-side-encryption s3 Para obtener más información, consulte Lista de reglas AWS Config administradas.	25 de enero de 2018
AWS Config admite el tipo de recurso Elastic Load Balancing	Con esta versión, puede utilizarla AWS Config para registrar los cambios de configuración en los balanceadores de carga clásicos de Elastic Load Balancing. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	17 de noviembre de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite Amazon CloudFront y el tipo AWS WAF de recurso	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en su CloudFront distribución y distribución en streaming. Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en los siguientes recursos AWS WAF y en los AWS WAF regionales: reglas basadas en tarifas, reglas y ACL web. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	15 de noviembre de 2017
AWS Config admite el tipo AWS CodeBuild de recurso	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración de sus AWS CodeBuild proyectos. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	20 de octubre de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite los recursos de Auto Scaling y una nueva regla administrada	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en los siguientes recursos de Auto Scaling: grupos, configuración de lanzamien to, acción programada y política de escalado. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config. Esta versión también admite la siguiente nueva regla administrada: • autoscaling-group-elb-healthcheck-obligatorio Para obtener más información, consulte AWS ConfigReglas de administradas.	18 de septiembre de 2017
AWS Config admite el tipo AWS CodeBuild de recurso	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración de sus AWS CodeBuild proyectos. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	20 de octubre de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite los recursos de Auto Scaling y una nueva regla administrada	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en los siguientes recursos de Auto Scaling: grupos, configuración de lanzamien to, acción programada y política de escalado. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config. Esta versión también admite la siguiente nueva regla administrada: • autoscaling-group-elb-healthcheck-obligatorio Para obtener más información, consulte AWS ConfigReglas de administradas.	18 de septiembre de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite el tipo de recurso de tabla DynamoDB y una nueva regla administrada	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en las tablas de DynamoDB. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config. Esta versión admite la siguiente nueva regla administrada: • dynamodb-autoscaling-enabled Para obtener más información, consulte AWS ConfigReglas de administradas.	8 de septiembre de 2017
AWS Config admite dos nuevas reglas administradas para Amazon S3	Esta versión admite dos nuevas reglas administradas: • s3- bucket-public-read-prohibited • s3- bucket-public-write-prohibited Para obtener más información, consulte AWS ConfigReglas de administradas.	14 de agosto de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
Nueva página en la AWS Config consola	Puede utilizar el panel de control de la AWS Config consola para ver lo siguiente: • La cantidad total de recursos • Cantidad total de reglas • Cantidad de recursos no conformes • Cantidad de reglas no conformes Para obtener más información, consulte Visualización del AWS Config panel.	17 de julio de 2017
Nueva operación API	Puede utilizar la GetDiscoveredResourceCountsoperación para obtener el número de tipos de recursos, el número de cada tipo de recurso y el número total de recursos que AWS Config se registran en una región para usted Cuenta de AWS.	17 de julio de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite el tipo de recurso de CloudFormation pila y una nueva regla gestionada	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en sus CloudFormation pilas. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config. Esta versión admite la siguiente nueva regla administrada: • cloudformation-stack-notification-check Para obtener más información, consulte AWS ConfigReglas de administradas.	6 de julio de 2017
Contenido nuevo y actualizado	Esta versión añade compatibilidad con las AWS Config reglas de la región de Canadá (centro) y la región de Sudamérica (São Paulo). Para ver todas las regiones que admiten AWS Config y Config Rules, consulte Regiones de AWS y Endpoints en. Referencia general de AWS	5 de julio de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
Contenido nuevo y actualizado	AWS Config Las reglas están disponibles en la AWS GovCloud (US) región. Para obtener más información, consulte la Guía del usuario de AWS GovCloud (US). Para ver las regiones compatibles AWS Config, consulte Regiones de AWS los puntos finales en. Referenci a general de AWS	8 de junio de 2017
AWS Config admite el tipo de recurso de CloudWatc h alarma de Amazon y tres nuevas reglas administradas	Con esta versión, puedes utilizarl a AWS Config para registrar los cambios de configuración de tus CloudWatch alarmas de Amazon. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config. Esta versión admite tres nuevas reglas administradas: • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check Para obtener más información, consulte AWS ConfigReglas de administradas.	1 de junio de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
Contenido nuevo y actualizado	Esta versión admite la especificación del número de versión de la aplicación para las siguientes reglas administradas: • ec-2 managedinstance-applications-blacklisted • ec-2 managedinstance-applications-required Para obtener más información, consulte AWS ConfigReglas de administradas.	1 de junio de 2017
Contenido nuevo y actualizado	Esta versión añade compatibilidad con las AWS Config reglas de la región de Asia Pacífico (Bombay). Para obtener más información, consulte Regiones de AWS and Endpoints en la Referencia general de AWS.	27 de abril de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
Contenido nuevo y actualizado	Esta versión admite una consola actualizada para añadir reglas administradas de AWS Config a su cuenta por primera vez. Cuando configuras AWS Config reglas por primera vez o en una nueva región, puedes buscar las reglas AWS administradas por nombre, descripción o etiqueta. Puede elegir Select all (Seleccio nar todas) para seleccionar todas las reglas o elegir Clear All (Borrar todas) para borrar todas las reglas. Para obtener más información, consulte Añadir, ver, actualizar y eliminar reglas (consola).	5 de abril de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite nuevas reglas administradas	Esta versión admite las nuevas reglas administradas que se indican a continuación: • acm-certificate-expiration-check • ec-2 instance-detailed-monitoring-enabled • ec-2 managedinstance-inventory-blacklisted • ec-2 volume-inuse-check • iam-user-group-membership-comprobar • iam-user-no-policies-comprobar • s3- bucket-ssl-requests-only Para obtener más información, consulte Lista de reglas AWS Config administradas.	21 de febrero de 2017
Contenido nuevo y actualizado	Esta versión añade compatibilidad con las AWS Config reglas de la región de Europa (Londres). Para obtener más información, consulte Regiones de AWS and Endpoints en la Referencia general de AWS.	21 de febrero de 2017

Cambio	Description (Descripción)	Fecha de lanzamiento
Contenido nuevo y actualizado	Esta versión añade CloudFormation plantillas para las reglas AWS Config gestionadas. Puede utilizar las plantillas para crear reglas administr adas para su cuenta. Para obtener más información, consulte Creación de reglas AWS Config administradas con AWS CloudFormation plantillas.	16 de febrero de 2017
Contenido nuevo y actualizado	Esta versión incorpora soporte para un nuevo modo de prueba para la API de `PutEvaluations` . Especifique el parámetro `TestMode` en true en la regla personalizada para verificar si la función AWS Lambda entregará los resultado s de la evaluación a AWS Config. No se producen actualizaciones en las evaluaciones existentes y los resultados de las evaluaciones no se envían a AWS Config. Para obtener más información, consulta PutEvaluations en la AWS Config Referencia de la API de .	16 de febrero de 2017
Contenido nuevo y actualizado	Esta versión añade compatibilidad con las AWS Config reglas de las regiones de Asia Pacífico (Seúl) y EE.UU. Oeste (norte de Californi a). Para obtener más información, consulte Regiones de AWS and Endpoints en la Referencia general de AWS.	21 de diciembre de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
Contenido nuevo y actualizado	Esta versión añade compatibilidad con AWS Config la región de Europa (Londres). Para obtener más información, consulte Regiones de AWS and Endpoints en la Referencia general de AWS.	13 de diciembre de 2016
Contenido nuevo y actualizado	Esta versión añade soporte para AWS Config la región de Canadá (Central). Para obtener más información, consulte Regiones de AWS and Endpoints en la Referencia general de AWS.	8 de diciembre de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite los tipos de recursos de Amazon Redshift y dos nuevas reglas administr adas	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración de sus clústeres de Amazon Redshift, grupos de parámetros de clúster, grupos de seguridad de clústeres, instantáneas de clústeres, grupos de subredes de clústeres y suscripci ones a eventos. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config. Esta versión admite dos nuevas reglas administradas: • redshift-cluster-configuration-check • redshift-cluster-maintenanc esettings-check Para obtener más información, consulte Lista de reglas AWS Config administradas.	7 de diciembre de 2016
Contenido nuevo y actualizado	Esta versión incorpora soporte para una nueva regla administrada: • dynamodb-throughput-limit-check Para obtener más información, consulte Lista de reglas AWS Config administradas.	7 de diciembre de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
Contenido nuevo y actualizado	Esta versión agrega compatibilidad para crear hasta 50 reglas por región en una cuenta. Para obtener más información, consulte Límites de AWS Config en la Referencia general de AWS.	7 de diciembre de 2016
AWS Config admite el tipo de recurso de inventario de instancias gestionadas para Amazon EC2 Systems Manager y tres nuevas reglas gestionadas	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración del software en las instancias administr adas con soporte para el inventario de instancias administradas. Para obtener más información, consulte Recording Software Configuration for Managed Instances. Esta versión admite tres nuevas reglas administradas: • ec-2 managedinstance-inventory-b lacklisted • ec-2 managedinstance-application s-required • ec-2 managedinstance-platform-ch eck Para obtener más información, consulte Lista de reglas AWS Config administradas.	1 de diciembre de 2016
Contenido nuevo y actualizado	AWS Config está disponible en la región China (Pekín).	24 de octubre de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite el recurso bucket de Amazon S3 y dos nuevas reglas administradas	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en sus buckets de Amazon S3. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config. Esta versión admite dos nuevas reglas administradas: • s3- bucket-logging-enabled • s3- bucket-versioning-enabled Para obtener más información, consulte AWS ConfigReglas de administradas.	18 de octubre de 2016
Contenido nuevo y actualizado	Esta versión añade compatibilidad AWS Config y AWS Config reglas para la región Este de EE. UU. (Ohio). Para obtener más informaci ón, consulte Regiones de AWS and Endpoints en la Referencia general de AWS.	17 de octubre de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
Reglas administradas nuevas y actualizadas	Esta actualización añade soporte para ocho nuevas reglas administradas: • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted Puede especificar varios valores de parámetros para las reglas siguientes: • desired-instance-tenancy • required-tags Para obtener más información, consulte Lista de reglas AWS Config administradas.	4 de octubre de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
Contenido nuevo y actualizado para la AWS Config consola	Esta actualización añade la posibilidad de ver la actividad de la AWS CloudTrail API en la AWS Config cronología. Si CloudTrail está registrando para su cuenta, puede ver los eventos de creación, actualización y eliminación de la API relacionados con los cambios de configuración de sus recursos. Para obtener más información, consulte Ver el historial de cumplimiento de sus AWS recursos con AWS Config.	06 de septiembre de 2016
AWS Config admite el tipo de recurso Elastic Load Balancing	Con esta versión, puede utilizar la AWS Config para registrar los cambios de configuración en los balanceadores de carga de la aplicación Elastic Load Balancing . Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	31 de agosto de 2016
Contenido nuevo y actualizado	Esta versión añade compatibilidad con las AWS Config reglas de las regiones de Asia Pacífico (Singapur) y Asia Pacífico (Sídney). Para obtener más información, consulte Regiones de AWS and Endpoints en la Referencia general de AWS.	18 de agosto de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
Contenido nuevo y actualizado para AWS Config las reglas	Esta actualización incorpora soporte para la creación de una regla que se puede activar mediante cambios de configuración y con la frecuencia periódica que se elija. Para obtener más información, consulte Componentes de una AWS Config regla. Esta actualización también incorpora soporte para evaluar manualmente los recursos con respecto a la regla y eliminar los resultados de la evaluación. Para obtener más información, consulte Evaluación de sus recursos con AWS Config reglas. Esta actualización también incorpora soporte para evaluar tipos de recursos adicionales con reglas personalizadas.	25 de julio de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config admite los tipos de recursos Amazon RDS y AWS Certificate Manager (ACM)	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en las instancias de base de datos de Amazon Relational Database Service (Amazon RDS), los grupos de seguridad de bases de datos, las instantáneas de bases de datos, los grupos de subredes de bases de datos y las suscripciones a eventos. También se puede utilizar AWS Config para registrar los cambios de configuración en los certificados proporcionados por ACM. Para obtener más información, consulte Tipos de recursos compatibl es para AWS Config.	21 de julio de 2016
Informaci ón actualiza da sobre la administración del registro de configuración	Esta actualización añade pasos para cambiar de nombre y eliminar el registro de configuración para Uso del registrador de configuración.	07 de julio de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
Creación simplificada de roles y políticas actualizadas	Con esta actualización, se simplific a la creación de un rol de IAM para AWS Config . Esta mejora está disponible en las regiones que admiten reglas de configuración. Para permitir esta mejora, se han actualizado los pasos de Configura ción de AWS Config con la consola, el ejemplo de política de Permisos del bucket de Amazon S3 para el canal AWS Config de entrega y el ejemplo de política de Ejemplos de políticas basadas en la identidad para AWS Config.	31 de marzo de 2016
Ejemplo de funciones y eventos de reglas de configuración	Esta actualización proporciona funciones de ejemplo actualizadas.	29 de marzo de 2016
AWS Config Repositorio de reglas GitHub	Esta actualización agrega informaci ón sobre el GitHub repositorio de AWS Config reglas aEvaluació n de recursos con AWS Config reglas. Este repositorio proporcio na ejemplos de funciones para reglas personalizadas desarrolladas y aportadas por AWS Config los usuarios.	1 de marzo de 2016

Cambio	Description (Descripción)	Fecha de lanzamiento
AWS Config Reglas	Esta versión presenta AWS Config las reglas. Las reglas se pueden utilizar AWS Config para evaluar si AWS los recursos cumplen con las configuraciones deseadas. Para obtener más información, consulte Evaluación de recursos con AWS Config reglas.	18 de diciembre de 2015
AWS Config admite los tipos de recursos de IAM	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración de sus usuarios, grupos, funciones y políticas gestionadas por los clientes de IAM. Para obtener más informaci ón, consulte Tipos de recursos compatibles para AWS Config.	10 de diciembre de 2015
AWS Config es compatible con el host dedicado de EC2	Con esta versión, puede utilizarl a AWS Config para registrar los cambios de configuración en sus hosts dedicados de EC2. Para obtener más información, consulte Tipos de recursos compatibles para AWS Config.	23 de noviembre de 2015

Cambio	Description (Descripción)	Fecha de lanzamiento
Información de permisos actualizada	Esta actualización agrega información sobre las siguientes políticas AWS administradas para AWS Config: • `AWS_ConfigRole` : concede permiso a AWS Config para obtener los detalles de la configuración sobre los recursos. Para obtener más información, consulte Política de roles de IAM para obtener datos de configuración. • `AWSConfigUserAccess` — Otorga acceso de solo lectura a un AWS Config usuario. Para obtener más información, consulte Acceso de solo lectura a AWS Config.	19 de octubre de 2015
AWS Config Vista previa de las reglas	Esta versión presenta la vista previa de AWS Config las reglas. Las reglas se pueden utilizar AWS Config para evaluar si AWS los recursos cumplen con las configuraciones deseadas. Para obtener más información, consulte Evaluación de recursos con AWS Config reglas.	7 de octubre de 2015
Contenido nuevo y actualizado	Esta versión añade la posibilidad de buscar los recursos que AWS Config haya descubierto. Para obtener más información, consulte Búsqueda de recursos descubiertos por AWS Config.	27 de agosto de 2015

Cambio	Description (Descripción)	Fecha de lanzamiento
Contenido nuevo y actualizado	Esta versión añade la posibilidad de seleccionar qué tipos de recursos registra AWS Config . Para obtener más información, consulte Grabación de AWS recursos con AWS Config.	23 de junio de 2015
Contenido nuevo y actualizado	Esta versión admite las siguiente s regiones: Asia Pacífico (Tokio), Asia Pacífico (Singapur), Europa (Fráncfort), América del Sur (São Paulo) y Oeste de EE. UU. (Norte de California). Para obtener más información, consulte Puntos de conexión y Regiones de AWS.	6 de abril de 2015
Nueva guía	Esta versión introduce AWS Config.	12 de noviembre de 2014

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.